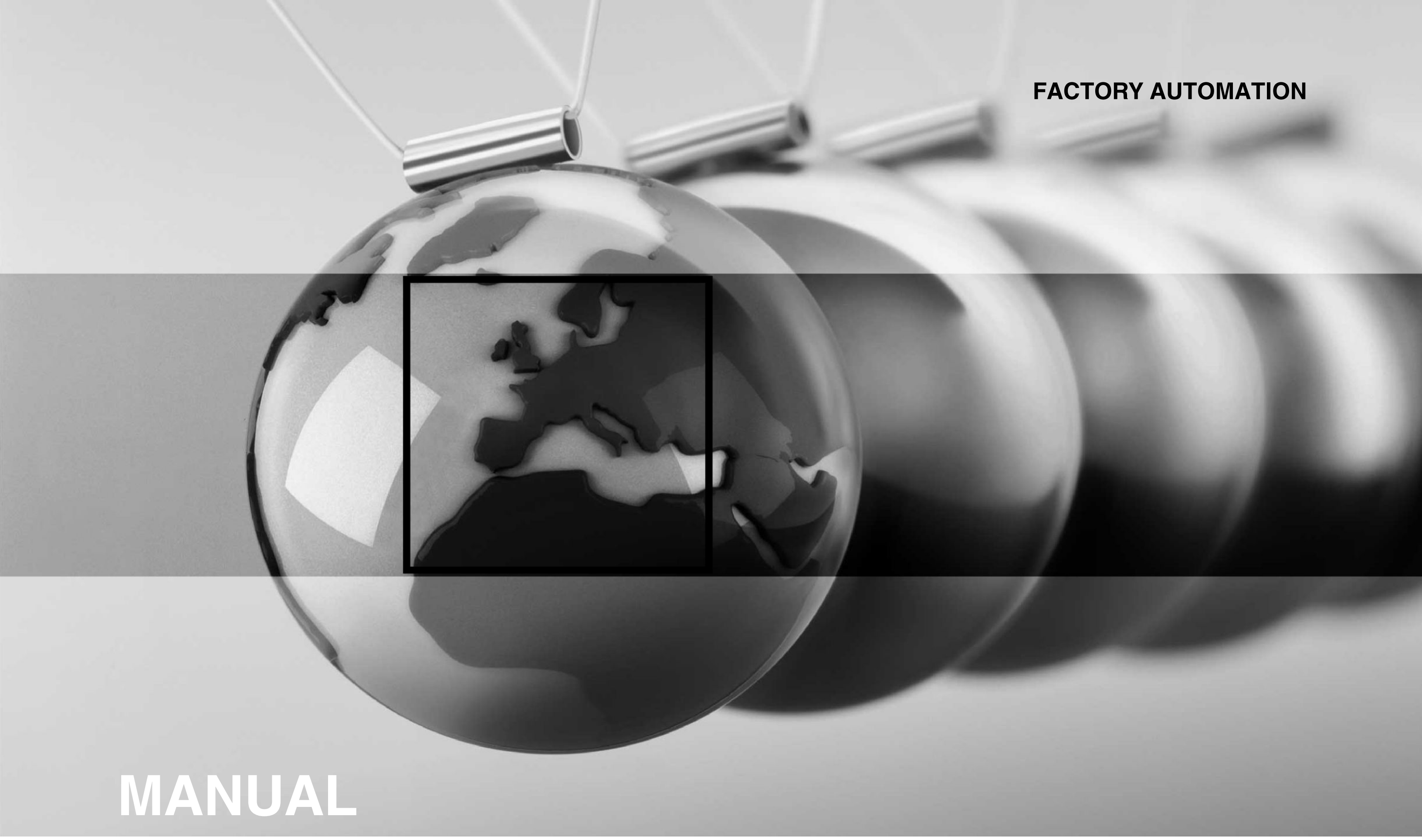
FACTORY AUTOMATION



ICDM-RX/TCP-16RJ45/ 2RJ45-PM

Hardware Installation and Configuration

PEPPERL+FUCHS
SENSING YOUR NEEDS

With regard to the supply of products, the current issue of the following document is applicable: The General Terms of Delivery for Products and Services of the Electrical Industry, published by the Central Association of the Electrical Industry (Zentralverband Elektrotechnik und Elektroindustrie (ZVEI) e.V.) in its most recent version as well as the supplementary clause: "Expanded reservation of proprietorship".

Table of Contents

1. ICDM-RX/TCP-16RJ45/2RJ45-PM Introduction

This section discusses the following topics:

- *ICDM-RX/TCP-16RJ45/2RJ45-PM Port Usage* (below)
- *Installation Overview* on Page 7
  - *NS-Link COM Port Driver Installation Overview* on Page 8
  - *NS-Link tty Port Installation Overview* on Page 8
  - *TCP/IP Socket Port Installation Overview* on Page 9
- *Locating Software and Documentation* on Page 9
- *Connectivity Requirements* on Page 9

1.1. ICDM-RX/TCP-16RJ45/2RJ45-PM Port Usage

ICDM-RX/TCP-16RJ45/2RJ45-PM serial ports can be configured for many environments, which include the following:

- *COM port* (or secure COM ports) when the NS-Link driver for Windows is installed
- *tty ports* when the NS-Link driver for Linux is installed
- *Socket ports* when SocketServer or the NS-Link web page is configured accordingly

1.2. Installation Overview

ICDM-RX/TCP-16RJ45/2RJ45-PM installation and configuration follows these steps:

1. Hardware installation.

   Power up the ICDM-RX/TCP-16RJ45/2RJ45-PM. Technical Support suggests installing one ICDM-RX/TCP-16RJ45/2RJ45-PM at a time to avoid configuration problems using *Hardware Installation* on Page 10.

2. Install PortVision DX.

   Pepperl+Fuchs recommends connecting the ICDM-RX/TCP-16RJ45/2RJ45-PM to a PC or laptop running Windows and that you install PortVision DX for easy IP address configuration and firmware updates. See *Installing PortVision DX* on Page 13 to install PortVision DX.

3. Program the IP address.

   See *Configuring the Network Settings (PortVision DX)* on Page 14 for detailed configuration procedures.

4. If necessary, update SocketServer, which can be downloaded from https://www.pepperl-fuchs.com.

   Note: *Technical Supports recommends that you update to the latest version of SocketServer before installing any NS-Link device driver or configuring socket ports.*

   a. Check the SocketServer version using *Checking the SocketServer Version* on Page 15 to determine the version on the ICDM-RX/TCP-16RJ45/2RJ45-PM.

   b. If necessary, update SocketServer. See *Uploading SocketServer with PortVision DX* on Page 16.

   Note: *In rare cases, you may need to update Bootloader to support a new feature. A notice will posted with SocketServer or the device driver if this is the case.*

5. Go to the appropriate overview or overviews for your installation:

   - NS-Link COM ports (or secure COM ports) - *NS-Link COM Port Driver Installation Overview* on Page 8
   - NS-Link tty ports - *NS-Link tty Port Installation Overview* on Page 8
   - TCP/IP socket ports - *TCP/IP Socket Port Installation Overview* on Page 9

1.2.1. NS-Link COM Port Driver Installation Overview

Use the following overview, which are discussed in detail in the subsequent sections, to install and configure the ICDM-RX/TCP-16RJ45/2RJ45-PM to run the NS-Link device driver for Windows operating systems..

1. After connecting the ICDM-RX/TCP-16RJ45/2RJ45-PM, programming the IP address with PortVision DX, and uploading the latest version of SocketServer, you are ready to install the driver.
2. Install the NS-Link device driver.

   See *Windows Installations* on Page 19 for an installation overview of the NS-Link driver for Windows operating systems and refer to the help system for more information.
3. Configure the COM ports using the *ICDM-RX/TCP-16RJ45/2RJ45-PM Windows Drivers Management Console*. See *Configuring the NS-Link Driver for Windows* on Page 20, which provides an overview of COM port configuration.
4. Configure device properties, you can refer to *Configuring COM Port Properties for Windows* on Page 26.
5. Optionally, you may need to configure one or more ports for socket mode. See *Socket Port Configuration* on Page 30 for information about configuring socket ports using the *Server Configuration* web page.
6. Connect the serial devices to the ICDM-RX/TCP-16RJ45/2RJ45-PM. Refer to on Page 76*Connecting Serial Devices* on Page 62 for cabling and connector information.

1.2.2. NS-Link tty Port Installation Overview

Use the following steps, which are discussed in detail in the subsequent sections, to install and configure the ICDM-RX/TCP-16RJ45/2RJ45-PM to run the NS-Link device driver for Linux operating systems.

1. After connecting the ICDM-RX/TCP-16RJ45/2RJ45-PM, programming the IP address, and uploading the latest version of SocketServer, you are ready to install the driver.
2. Locate and unpackage the driver assembly at https://www.pepperl-fuchs.com.

   Refer to the **readme** file packaged with the Linux driver assembly for driver installation and configuration procedures for the tty port.
3. Optionally, you may need to configure one or more ports for socket mode. See *Socket Port Configuration* on Page 30 for information about configuring socket ports using the web interface (SocketServer/NS-Link).
4. Connect the serial devices to the ICDM-RX/TCP-16RJ45/2RJ45-PM. Refer to on Page 76*Connecting Serial Devices* on Page 62 for cabling and connector information.

1.2.3. TCP/IP Socket Port Installation Overview

Use the following steps, which are discussed in detail in the subsequent sections, to configure ICDM-RX/TCP-16RJ45/2RJ45-PM socket ports.

1. After connecting the ICDM-RX/TCP-16RJ45/2RJ45-PM, programming the IP address, and uploading the latest version of SocketServer, you are ready to configure socket port or serial tunneling.
2. Configure the serial socket ports using the PortVision DX property pages or enter the IP address in a web browser and use the SocketServer web pages.

   You can refer to the SocketServer help system or *Socket Port Configuration* on Page 30 for information for configuration procedures.
3. Connect the serial devices to the ICDM-RX/TCP-16RJ45/2RJ45-PM. Refer to on Page 76*Connecting Serial Devices* on Page 62 for cabling and connector information.

1.3. Locating Software and Documentation

You can access the appropriate software assembly (firmware and drivers), PortVision DX, and ICDM-RX/TCP-16RJ45/2RJ45-PM documentation at: https://www.pepperl-fuchs.com.

1.4. Connectivity Requirements

An Ethernet connection: either to an Ethernet hub, switch, or router; or to a Network Interface Card (NIC) in the host system using a standard Ethernet cable.

2. Hardware Installation

Use the following procedure to install the ICDM-RX/TCP-16RJ45/2RJ45-PM with an external power supply.

1. Place the ICDM-RX/TCP-16RJ45/2RJ45-PM on a stable surface.

   Note: *Do not connect multiple units until you have changed the default IP address, see Initial Configuration on Page 12.*

2. Connect the ICDM-RX/TCP-16RJ45/2RJ45-PM to the same Ethernet network segment as the host PC using either port labeled **10/100** using a standard Ethernet cable.

   ⚠ Caution ***Do not connect RS-422/485 devices until the appropriate port interface type has been configured. The default port setting is RS-232.***

3. Apply power to the ICDM-RX/TCP-16RJ45/2RJ45-PM by connecting the AC power adapter to the ICDM-RX/TCP-16RJ45/2RJ45-PM, the power cord to the power adapter, and plugging the power cord into a power source. See *External Power Supply Specifications* on Page 97 if you want to provide your own power supply.

4. Verify that the **STAT** LED has completed the boot cycle and network connection for the ICDM-RX/TCP-16RJ45/2RJ45-PM is functioning properly.

   Note: *The RX/TX LEDs cycle during a reboot.*

   - **STAT** (Status LED) - If the Status LED on the DeviceMaster LT is lit, it indicates the ICDM-RX/TCP-16RJ45/2RJ45-PM has power and it has completed the boot cycle.

     The **STAT** LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.

   - Ethernet LEDs - The green LED indicates that a link has been established and the yellow LED indicates activity.

5. Go to *Initial Configuration* on Page 12 for default network settings and how to configure the ICDM-RX/TCP-16RJ45/2RJ45-PM for use.

3. Initial Configuration

There are several ways to configure network information. Pepperl+Fuchs Technical Support recommends connecting the ICDM-RX/TCP-16RJ45/2RJ45-PM to a PC or laptop running Windows and installing *PortVision DX* for initial configuration.

Optionally, you can use RedBoot to configure the network address, see *RedBoot Procedures* on Page 88.

This section shows how to use PortVision DX for initial ICDM-RX/TCP-16RJ45/2RJ45-PM configuration. It also defines requirements and how configuring ICDM-RX/TCP-16RJ45/2RJ45-PM security affects PortVision DX and shows you how to:

- Install PortVision DX
- Configure the network address (Page 14)
- Check the SocketServer version on the ICDM-RX/TCP-16RJ45/2RJ45-PM (Page 15)
- If necessary, upload the latest SocketServer version into the ICDM-RX/TCP-16RJ45/2RJ45-PM (Page 16)

3.1. PortVision DX Overview

PortVision DX automatically detects Pepperl+Fuchs ICDM-RX, ICE2, ICE3 or ICRL Ethernet attached products physically attached to the local network segment so that you can configure the network address, upload firmware, and manage the following products:

- ICDM-RX family
- IO-Link master (ICE2/ICE3)
- RocketLinx managed switches

In addition to identifying Pepperl+Fuchs ICDM-RX, ICE2, ICE3 or ICRL Ethernet attached products, you can use PortVision DX to display any third-party switch and hardware that may be connected directly to those devices. All non-Pepperl+Fuchs products and unmanaged RocketLinx switches are treated as non-intelligent devices and have limited feature support. For example, you cannot configure or update firmware on a third-party switch.

You can customize how PortVision DX displays the devices, refer to the **help** system for specific procedures.

- Create sessions tailored for specific audiences using the **New Session** and **Import Session** options.
- Sort by Device Name, Model, IP Address, MAC Address, Software Version or Status by clicking in the column heading to find devices faster.
- To create a spreadsheet of the information, use the **Export Device List to Notepad** option and then import it into your favorite spreadsheet. The text file is tab delimited.
- Organize all of your devices in logical folders as shown below.
- Add shortcuts to other applications using **Tools > Applications > Customize** feature.

3.2. PortVision DX Requirements

Use PortVision DX to identify, configure, update, and manage the ICDM-RX/TCP-16RJ45/2RJ45-PM on Windows Server 2008 R2 through Windows 11 operating systems.

PortVision DX requires that you connect the Pepperl+Fuchs ICDM-RX, ICE2, ICE3 or ICRL Ethernet attached product to the same network segment as the Windows host system if you want to be able to scan and locate it automatically during the configuration process.

3.3. Configuring Security Settings and PortVision DX

The following list provides basic PortVision DX operations that are affected how the ICDM-RX/TCP-16RJ45/2RJ45-PM interacts with PortVision DX when security is enabled using the web interface (SocketServer/NS-Link).

- PortVision DX must scan the ICDM-RX/TCP-16RJ45/2RJ45-PM *before* configuring security.
- PortVision DX locates the ICDM-RX/TCP-16RJ45/2RJ45-PM before setting either **Secure Data Mode** or **Secure Config Mode**.
- If PortVision DX discovers the ICDM-RX/TCP-16RJ45/2RJ45-PM *after* setting security, the following conditions occur:
  - A lock symbol displays before the Device Name.
  - The IP address of the ICDM-RX/TCP-16RJ45/2RJ45-PM does not display.
  - The *Software Settings* and *Web Interface* tabs are not present in the *Properties* page.
  - The IP mode displays as DHCP without the ability to modify.
  - The **Upload** and **Reboot** icons on the *Launch Bar* are grayed out and the options are disabled in the popup menus.

Note: *If the ICDM-RX/TCP-16RJ45/2RJ45-PM was previously configured with security, PortVision DX features are reduced.*

3.4. Installing PortVision DX

During initial configuration, PortVision DX automatically detects and identifies ICDM-RX/TCP-16RJ45/2RJ45-PM units, if they are in the same network segment.

1. Download PortVision DX from https://www.pepperl-fuchs.com.

   Note: *Depending on your operating system, you may need to respond to a Security Warning to permit access.*
2. Execute the **PortVision_DX[version].msi** file.
3. Click **Next** on the *Welcome* screen.
4. Click **I accept the terms in the License Agreement** and **Next**.
5. Click **Next** or optionally, browse to a different location and then click **Next**.
6. Click **Next** to configure the shortcuts.
7. Click **Install**.
8. Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to install software on this computer?* query.
9. Click **Launch PortVision DX** and **Finish** in the last installation screen.

10. Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* query.
11. Select the Pepperl+Fuchs ICDM-RX, ICE2, ICE3 or ICRL Ethernet attached products that you want to locate and then click **Scan**.

    Note: *If the Pepperl+Fuchs ICDM-RX, ICE2, ICE3 or ICRL Ethernet attached product is not on the local segment and it has been programmed with an IP address, it will be necessary to manually add the Pepperl+Fuchs ICDM-RX, ICE2, ICE3 or ICRL Ethernet attached product to PortVision DX. Refer to the PortVision DX for the procedure to manually add an ICDM-RX/TCP-16RJ45/2RJ45-PM.*
12. Go to Step 6 in the next section, *Configuring the Network Settings (PortVision DX)* on Page 14, to program the ICDM-RX/TCP-16RJ45/2RJ45-PM network settings.

You can customize how PortVision DX displays the devices, refer to the **help** system for specific procedures.

- Create sessions tailored for specific audiences using the **New Session** and **Import Session** options.
- Sort by Device Name, Model, IP Address, MAC Address, Software Version or Status by clicking in the column heading to find devices faster.
- To create a spreadsheet of the information, use the **Export Device List to Notepad** option and then import it into your favorite spreadsheet. The text file is tab delimited.
- Organize all of your devices in logical folders as shown below.
- Add shortcuts to other applications using **Tools** > **Applications** > **Customize** feature.

3.5. Configuring the Network Settings (PortVision DX)

Use the following procedure to change the default network settings on the ICDM-RX/TCP-16RJ45/2RJ45-PM for your network using PortVision DX. The default network settings are:

- IP address: 192.168.250.250
- Subnet mask: 255.255.0.0
- Gateway address: 192.168.250.1

Note: *Technical Support advises configuring one new ICDM-RX/TCP-16RJ45/2RJ45-PM at a time to avoid device driver configuration problems. If you want to configure multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs using the* ***Assign IP to Multiple Devices*** *option, see Configuring Multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs Network Addresses on Page 67.*

The following procedure shows how to configure a single ICDM-RX/TCP-16RJ45/2RJ45-PM connected to the same network segment as the Windows system. If the ICDM-RX/TCP-16RJ45/2RJ45-PM is not on the same physical segment, you can add it manually using *Adding a New Device in PortVision DX* on Page 67.

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 13).
2. Start PortVision DX using the **PortVision DX** desktop shortcut or from the **Start** button, click **Pepperl+Fuchs Comtrol** > **PortVision DX**.
3. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* query.
4. Click the **Scan** button in the *Toolbar*.
5. Click **Scan** to locate the Pepperl+Fuchs ICDM-RX, ICE2, ICE3 or ICRL Ethernet attached products including the ICDM-RX/TCP-16RJ45/2RJ45-PM on the network.

    Note: *If you do not have any RocketLinx managed switches or IO-Link master (ICE2/ICE3)s, it saves scanning time if you do not scan for them.*

    If PortVision DX does not locate your ICDM-RX/TCP-16RJ45/2RJ45-PM on the network, make sure that you are using the latest version of PortVision DX: https://www.pepperl-fuchs.com.
6. Right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM and select **Properties** in the pop up menu.
7. *Optionally*, rename the ICDM-RX/TCP-16RJ45/2RJ45-PM in the **Device Name** field.

Note: *The MAC address, Serial Number and Device Status fields are automatically populated and you cannot change those values.*

8. Optionally, enter the serial number, which is on a label on the ICDM-RX/TCP-16RJ45/2RJ45-PM.
9. If necessary, you can change the **Detection Type**.
   - **REMOTE** means that the ICDM-RX/TCP-16RJ45/2RJ45-PM is not connected to this segment of the network and it uses IP communications, not MAC communications.
   - **LOCAL** means that the ICDM-RX/TCP-16RJ45/2RJ45-PM is on this local network segment and uses MAC communications. An IP address is not required but Technical support recommends using an IP address.
10. Change the ICDM-RX/TCP-16RJ45/2RJ45-PM network properties as required for your site.
    - To use the ICDM-RX/TCP-16RJ45/2RJ45-PM with DHCP, click **DHCP IP**, and make sure that you provide the MAC address of the device to the network administrator. Make sure that the administrator reserves the IP address, subnet mask and gateway address of the ICDM-RX/TCP-16RJ45/2RJ45-PM in the DHCP server.
    - To program a static IP address, click **Static IP** and enter the appropriate values for your site.

    Note: *For additional information, open the PortVision DX Help system.*
11. Typically, the **Bootloader Timeout** value should be left to it's default value. In some situations, you may need to temporarily adjust the **Bootloader Timeout** to a higher value during a firmware update.
12. Click **Apply Changes** to update the network information on the ICDM-RX/TCP-16RJ45/2RJ45-PM.

    Note: *If you are deploying multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs that share common values, you can save the configuration file and load that configuration onto other ICDM-RX/TCP-16RJ45/2RJ45-PMs. See Using SocketServer Configuration Files on Page 69 for more information.*
13. Click **Close** to exit the *Properties* window.

Go to *Checking the SocketServer Version* on Page 15 to check the SocketServer version. You should update SocketServer firmware before any further configuration.

3.6. Checking the SocketServer Version

SocketServer refers to the web page that is integrated in the firmware that comes pre-installed on your ICDM-RX/TCP-16RJ45/2RJ45-PM platform, which provides an interface to TCP/IP socket mode configuration and services. If you install an NS-Link device driver, an NS-Link version of SocketServer loads on the ICDM-RX/TCP-16RJ45/2RJ45-PM.

Note: *Technical Support recommends that you update to the latest version of SocketServer before installing an NS-Link device driver or configuring socket ports.*

Use the following procedure to check the SocketServer version on the ICDM-RX/TCP-16RJ45/2RJ45-PM. .

1. If necessary, open PortVision DX **(Pepperl+Fuchs Comtrol > PortVision DX)** or use the desktop shortcut and scan the network.
2. Check the SocketServer version number of the *Software Version* for the ICDM-RX/TCP-16RJ45/2RJ45-PM.
3. Contact technical support at https://www.pepperl-fuchs.com to see if a later version of SocketServer is available.
4. If necessary, use *Uploading SocketServer with PortVision DX* on Page 16 to upload the latest version.

   If the SocketServer version on the ICDM-RX/TCP-16RJ45/2RJ45-PM is current, you are ready to continue the installation and configuration process.
   - *Device Driver (NS-Link) Installation* on Page 17
   - *Socket Port Configuration* on Page 30

3.7. Uploading SocketServer with PortVision DX

Use this section to upload a newer version of SocketServer on the ICDM-RX/TCP-16RJ45/2RJ45-PM using PortVision DX. Technical Support recommends updating SocketServer before any further configuration to avoid configuration problems.

You can use this procedure if your ICDM-RX/TCP-16RJ45/2RJ45-PM is connected to the host PC, laptop, or if the ICDM-RX/TCP-16RJ45/2RJ45-PM resides on the local network segment.

1. Unzip the file to locate the **.cmtl** file.
2. If necessary, open PortVision DX or use the desktop shortcut.
3. Right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM or ICDM-RX/TCP-16RJ45/2RJ45-PMs for which you want to update, click **Advanced > Upload Firmware**, browse to the SocketServer **.cmtl** file, and then click **Open**.

   If the **Detection Type** is set to **REMOTE**, you may want to change it to **LOCAL**.
4. Click **Yes** to the *Upload Firmware* message that warns you that this is a sensitive process. It may take a few moments for the firmware to upload onto the ICDM-RX/TCP-16RJ45/2RJ45-PM. The ICDM-RX/TCP-16RJ45/2RJ45-PM reboots itself during the upload process.
5. Click **Ok** to the advisory message about waiting to use the device until the status reads **ON-LINE**. In the next polling cycle, PortVision DX updates displays the new SocketServer version or depending your polling settings, click the **Refresh** button.
6. If the upload fails, reset the Bootloader timeout to 60 seconds and then repeat Steps 3 through 5. For procedures, see *Changing the Bootloader Timeout* on Page 75.

You are now ready to continue the installation and configuration process.

- *Device Driver (NS-Link) Installation* on Page 17
- *Socket Port Configuration* on Page 30

4. Device Driver (NS-Link) Installation

This section discusses the following topics:

- *Linux Installations* on Page 18
- *Windows Installations* on Page 19

4.1. Overview

The following subsections discuss procedures that need to be done before installing and configuring the NS-Link device driver.

4.1.1. Before Installing the NS-Link Driver

Before installing the NS-Link device driver for the Linux and Windows operating systems, the following conditions must be met:

- The ICDM-RX/TCP-16RJ45/2RJ45-PM is connected to the network and powered on (*Hardware Installation* on Page 10).
- The network information has been configured in the ICDM-RX/TCP-16RJ45/2RJ45-PM (*Configuring the Network Settings (PortVision DX)* on Page 14).
- Checked to see if the latest version of SocketServer resides on the ICDM-RX/TCP-16RJ45/2RJ45-PM (*Checking the SocketServer Version* on Page 15 using PortVision DX or you can open your browser, enter the ICDM-RX/TCP-16RJ45/2RJ45-PM IP address to view the version on the *Server Status* page.
- If necessary, uploaded the latest version of SocketServer (*Uploading SocketServer with PortVision DX* on Page 16.

Note: *Technical Supports recommends that you update to the latest version of SocketServer before installing any NS-Link device driver.*

After NS-Link driver installation and configuration, the same ports can be configured as TCP/IP sockets using an NS-Link version of the SocketServer web page (*Socket Port Configuration* on Page 30).

4.2. Linux Installations

Download the latest device driver for Linux: https://www.pepperl-fuchs.com.

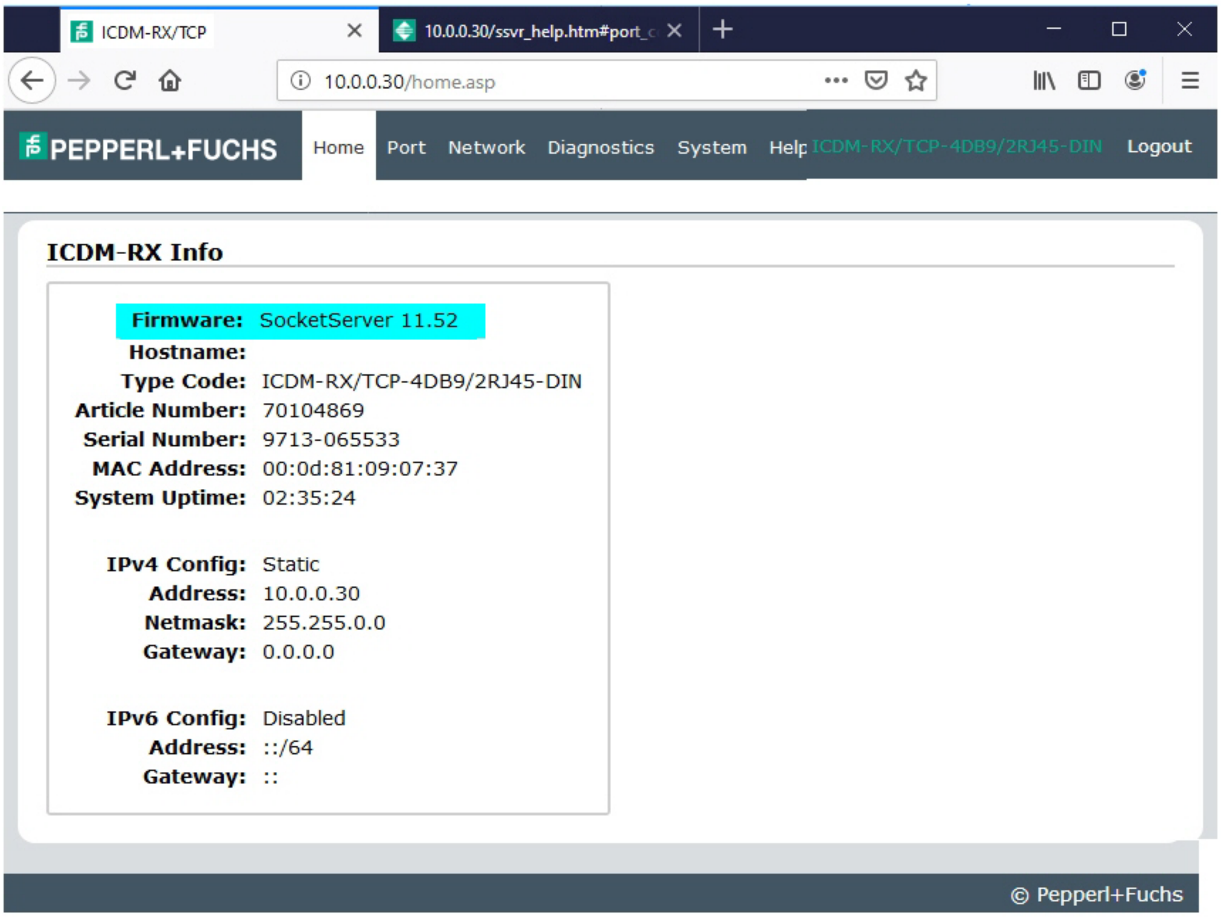
Refer to the **README** file packaged with the Linux driver for driver installation and configuration procedures.

Before you install the Linux NS-Link device driver:

1. Make sure that you have programmed an appropriate network address into the ICDM-RX/TCP-16RJ45/2RJ45-PM.
2. Make sure that you verify that you have the latest version of SocketServer loaded on the ICDM-RX/TCP-16RJ45/2RJ45-PM.
3. Open SocketServer to check the version by opening your browser and entering the IP address of the ICDM-RX/TCP-16RJ45/2RJ45-PM.
4. Contact Technical Support at https://www.pepperl-fuchs.com to check for the latest SocketServer version.
5. If necessary, upload the latest version.

Note: *Technical Supports recommends that you update to the latest version of SocketServer before installing an NS-Link device driver.*

6. Install and configure the Linux device driver using the **Readme** file packaged with the driver.



ICDM-RX Info

Firmware: SocketServer 11.52
Hostname:
Type Code: ICDM-RX/TCP-4DB9/2RJ45-DIN
Article Number: 70104869
Serial Number: 9713-065533
MAC Address: 00:0d:81:09:07:37
System Uptime: 02:35:24

IPv4 Config: Static
Address: 10.0.0.30
Netmask: 255.255.0.0
Gateway: 0.0.0.0

IPv6 Config: Disabled
Address: ::/64
Gateway: ::

© Pepperl+Fuchs

4.3. Windows Installations

This subsection provides an installation overview for the NS-Link device driver for Windows. For detailed installation and configuration information, see the ICDM-RX/TCP Device Driver (NS-Link) help system.

4.3.1. Supported Operating Systems

The NS-Link device driver for Windows supports Windows 2008 R2 through Windows 11 and Windows Server 2019.

If you are updating the driver or need to remove the NS-Link device driver, you can refer to the help system.

Note: *Administrative privileges are required to install device drivers on Windows systems.*

4.3.2. Installation Overview for Windows

The following NS-Link device driver installation and configuration procedures are discussed in this subsection:

- Install the NS-Link device driver and *ICDM-RX/TCP Windows Drivers Management Console* using the *Installation Wizard*.
- Configure the COM ports using the *Windows Drivers Management Console*.
- Configure device properties using the *Windows Drivers Management Console*.

4.3.3. NS-Link for Windows Installation

1. Locate the NS-Link device driver and make it available to the host system. The driver assembly is available at: https://www.pepperl-fuchs.com.
2. Unzip the file and then execute the driver assembly **DeviceMaster_ICDM-RX_Driver_x.xx.exe** file and click **Next** to start the installation.
3. Click **Yes** to the *Do you want to allow this app to make changes to your device?* screen.
4. Click **Next** to install in the default location.
5. Click **Install**.
6. Leave the **Launch ICDM-RX Driver Installation** box checked.

   If you do not check this box, you can use the shortcut under the **Start** button at: **Pepperl+Fuchs > ICDM-RX Driver Installation Wizard**.
7. Click **Finish** to complete the installation of the wizard.
8. Click **Next** to start the driver installation.
9. Click **Install** and **Next**.
10. Select the ICDM-RX/TCP model that you are installing from the list.
11. Enter the quantity of this ICDM-RX/TCP model that you want to install and click **Ok**.
12. Repeat Steps 10 and 11 for each ICDM-RX/TCP that you are installing and then click **Next**.
13. Click **Next**.
14. Click **Proceed**.

    You may see the popup at the right for each port, depending on the operating system.
15. If this is a self-certified driver, click the **Install** button..
16. Return to the *Installation Wizard* and click **Close**.

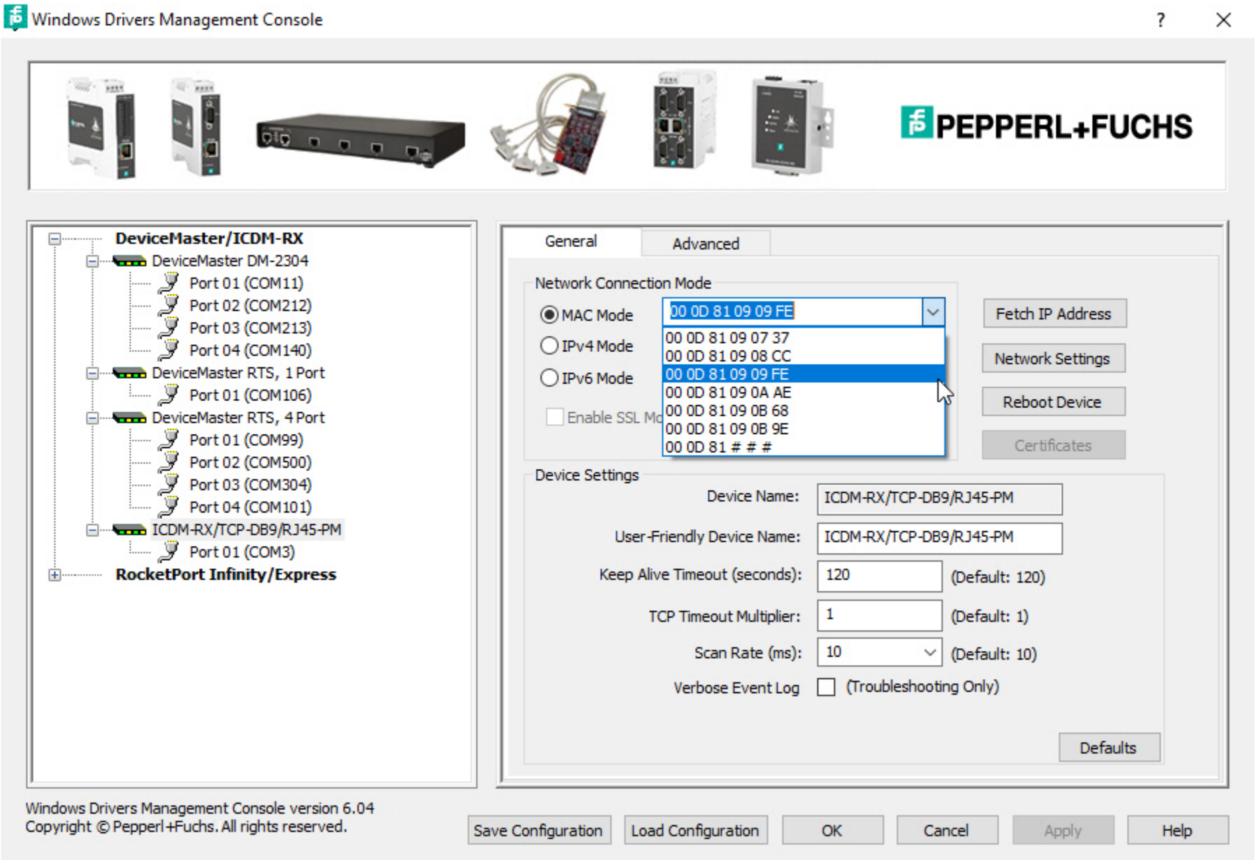
17. Go to the next subsection for NS-Link driver configuration procedures.

4.4. Configuring the NS-Link Driver for Windows

This subsection provides a configuration overview for the NS-Link driver. For detailed information or if the ICDM-RX/TCP-16RJ45/2RJ45-PM is on a different physical segment, refer to the help system.

The ICDM-RX/TCP-16RJ45/2RJ45-PM must be connected to the local network segment or directly to a NIC on the host system to operate in MAC mode to perform the following configuration steps.

1. Access the *Windows Drivers Management Console* using the desktop shortcut or under the start menu **> Pepperl+Fuchs Comtrol>Windows Driver Management Console**.
2. Highlight the *Device Name* of the ICDM-RX/TCP-16RJ45/2RJ45-PM that you want to configure.
3. Select the MAC address from the drop-down list or enter the address from the MAC address label on the ICDM-RX/TCP-16RJ45/2RJ45-PM. If you programmed the IP address using PortVision DX, the IP address displays in the **IP Mode** text box after you select the MAC address.



Network Connection Mode

● MAC Mode: 00 0D 81 09 09 FE

○ IPv4 Mode

○ IPv6 Mode

□ Enable SSL Mo

00 0D 81 09 07 37
00 0D 81 09 08 CC
00 0D 81 09 09 FE
00 0D 81 09 0A AE
00 0D 81 09 0B 68
00 0D 81 09 0B 9E
00 0D 81 # # #

Device Settings

Device Name:	ICDM-RX/TCP-DB9/RJ45-PM	
User-Friendly Device Name:	ICDM-RX/TCP-DB9/RJ45-PM	
Keep Alive Timeout (seconds):	120	(Default: 120)
TCP Timeout Multiplier:	1	(Default: 1)
Scan Rate (ms):	10	(Default: 10)
Verbose Event Log	□	(Troubleshooting Only)

Windows Drivers Management Console version 6.04
Copyright © Pepperl+Fuchs. All rights reserved.

Note: *If you enter the MAC address, make sure that you use the correct format, for example:* **00 C0 4E xx xx xx** *or* **00 0D 81 xx xx xx**. *A space must separate each pair of digits. The MAC address is located on a label on the ICDM-RX/TCP-16RJ45/2RJ45-PM or you can view it using PortVision DX.*

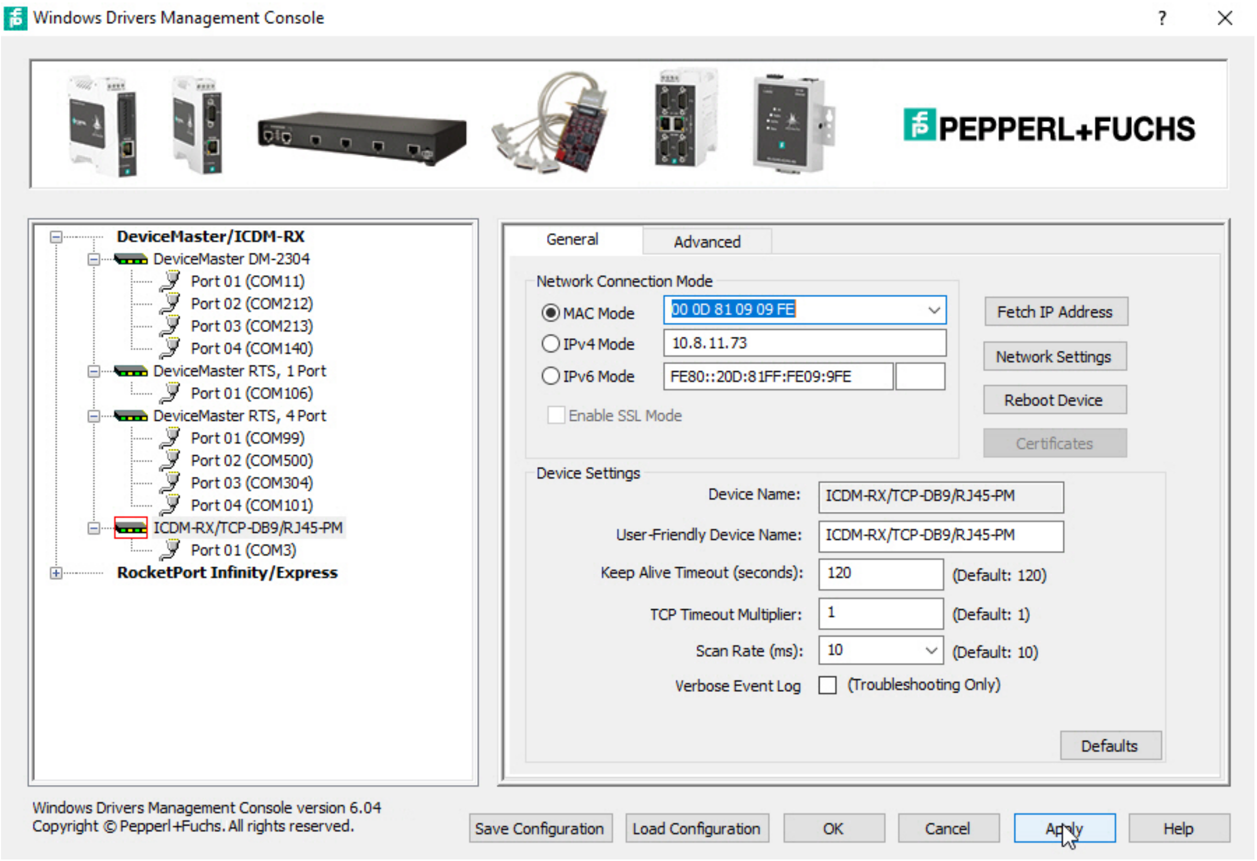
If the appropriate MAC address is not displayed in the drop-down list, then it can be one of the following reasons:

- Not on the same network segment
- ICDM-RX/TCP-16RJ45/2RJ45-PM not powered on or connected

- The wrong ICDM-RX model was selected during the driver installation
- Device failure

4. Click **Apply** to program the driver with the MAC address of the ICDM-RX/TCP-16RJ45/2RJ45-PM or **Ok** to save the change and close the *Windows Drivers Management Console*.

   If you do not **Apply** the changes before leaving this screen, you will be prompted to **Apply**, **Ignore**, or **Cancel** the changes.



Windows Drivers Management Console

DeviceMaster/ICDM-RX
- DeviceMaster DM-2304
  - Port 01 (COM11)
  - Port 02 (COM212)
  - Port 03 (COM213)
  - Port 04 (COM140)
- DeviceMaster RTS, 1 Port
  - Port 01 (COM106)
- DeviceMaster RTS, 4 Port
  - Port 01 (COM99)
  - Port 02 (COM500)
  - Port 03 (COM304)
  - Port 04 (COM101)
- ICDM-RX/TCP-DB9/RJ45-PM
  - Port 01 (COM3)

RocketPort Infinity/Express

General | Advanced

Network Connection Mode

● MAC Mode: 00 0D 81 09 09 FE
○ IPv4 Mode: 10.8.11.73
○ IPv6 Mode: FE80::20D:81FF:FE09:9FE
□ Enable SSL Mode

Device Settings

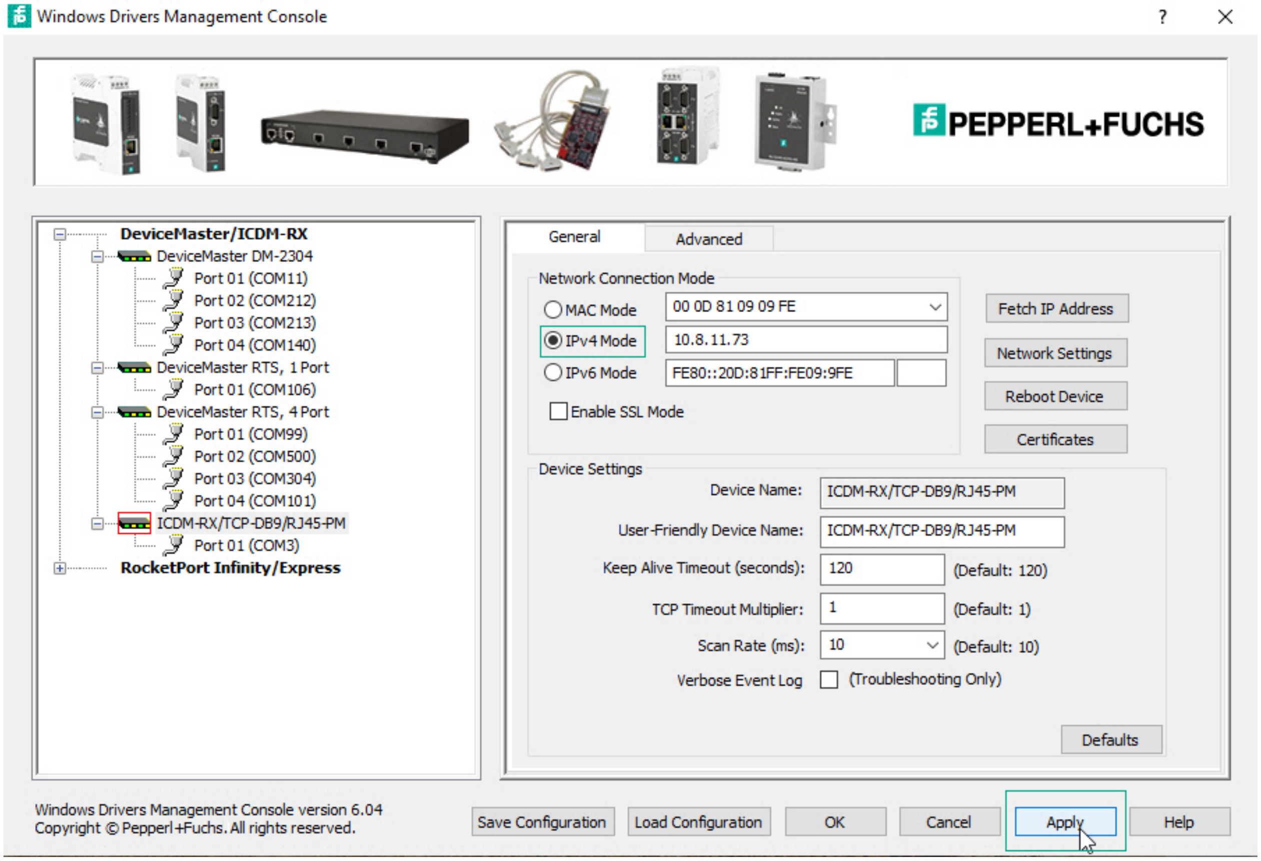
Device Name: ICDM-RX/TCP-DB9/RJ45-PM
User-Friendly Device Name: ICDM-RX/TCP-DB9/RJ45-PM
Keep Alive Timeout (seconds): 120 (Default: 120)
TCP Timeout Multiplier: 1 (Default: 1)
Scan Rate (ms): 10 (Default: 10)
Verbose Event Log □ (Troubleshooting Only)

Windows Drivers Management Console version 6.04
Copyright © Pepperl+Fuchs. All rights reserved.

Note: *The red frame around the selection indicates that the Apply button has not been executed.*

- Now that the MAC address has been associated to the ICDM-RX/TCP-16RJ45/2RJ45-PM, you can use the **Network Settings** screen to:
  - Change the IP address, set the ICDM-RX/TCP-16RJ45/2RJ45-PM to **DHCP**, or **Disable IP** communications using the **Network Settings** button
  - Reboot the ICDM-RX/TCP-16RJ45/2RJ45-PM on the **General** tab
  - Access network statistics on the **Advanced** tab

5. If you want use **IP mode** and the IP address is configured for your network, click the **IPv4** or **IPv6 Mode** radio button and click **Apply**. If you want to use **SSL Mode**, you must set the ICDM-RX/TCP-16RJ45/2RJ45-PM to **IP mode**.


Windows Drivers Management Console

- DeviceMaster/ICDM-RX
  - DeviceMaster DM-2304
    - Port 01 (COM11)
    - Port 02 (COM212)
    - Port 03 (COM213)
    - Port 04 (COM140)
  - DeviceMaster RTS, 1 Port
    - Port 01 (COM106)
  - DeviceMaster RTS, 4 Port
    - Port 01 (COM99)
    - Port 02 (COM500)
    - Port 03 (COM304)
    - Port 04 (COM101)
  - ICDM-RX/TCP-DB9/RJ45-PM
    - Port 01 (COM3)
- RocketPort Infinity/Express

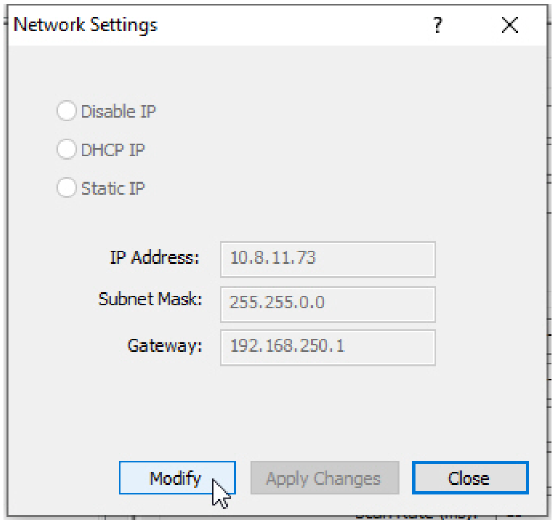
General | Advanced

Network Connection Mode
○ MAC Mode: 00 0D 81 09 09 FE
● IPv4 Mode: 10.8.11.73
○ IPv6 Mode: FE80::20D:81FF:FE09:9FE
□ Enable SSL Mode

Device Settings
Device Name: ICDM-RX/TCP-DB9/RJ45-PM
User-Friendly Device Name: ICDM-RX/TCP-DB9/RJ45-PM
Keep Alive Timeout (seconds): 120 (Default: 120)
TCP Timeout Multiplier: 1 (Default: 1)
Scan Rate (ms): 10 (Default: 10)
Verbose Event Log □ (Troubleshooting Only)

Windows Drivers Management Console version 6.04
Copyright © Pepperl+Fuchs. All rights reserved.

6. Optionally, click the **Network Settings** button and click **Modify** to make any network settings changes for DHCP or MAC mode (Disable IP).


Network Settings

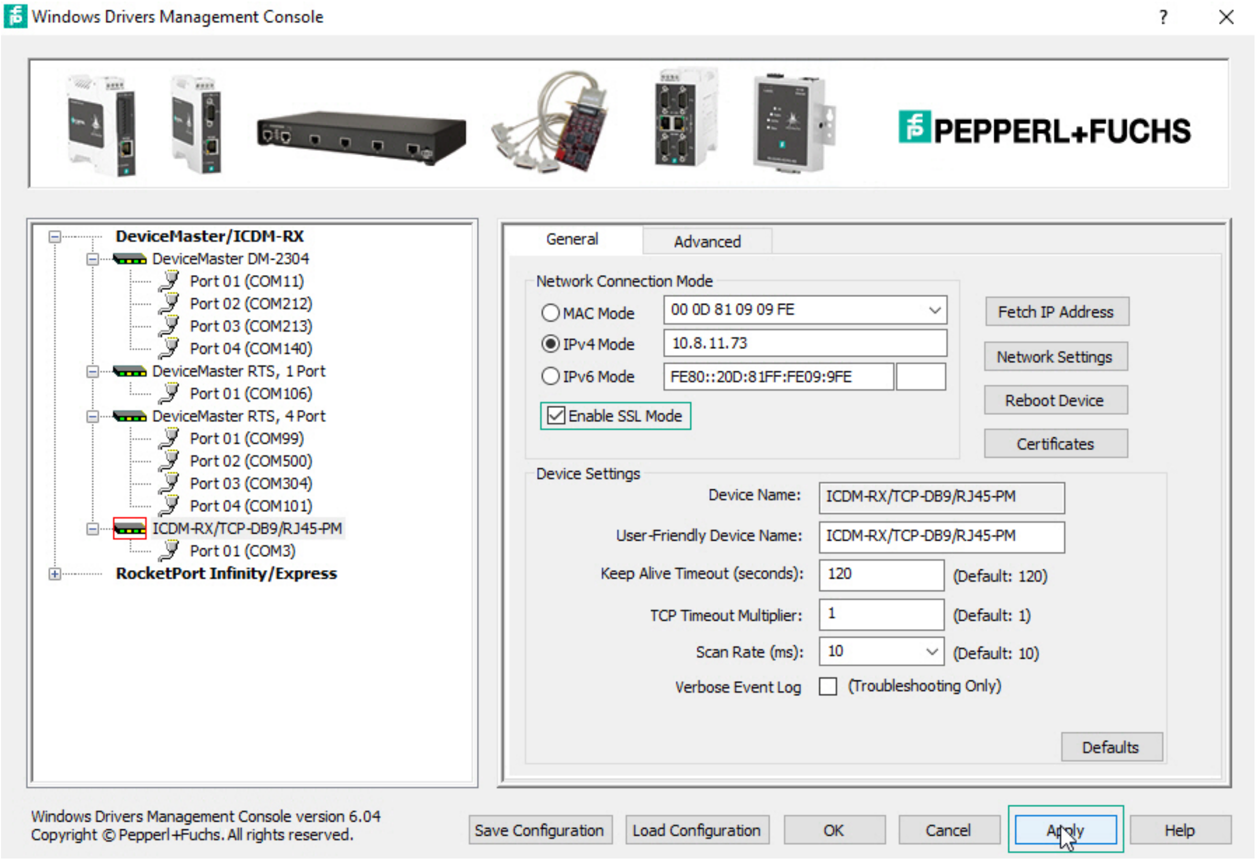
○ Disable IP
○ DHCP IP
○ Static IP

IP Address: 10.8.11.73
Subnet Mask: 255.255.0.0
Gateway: 192.168.250.1

a. Select the appropriate setting and if necessary, enter the IP Address, Subnet Mask and Gateway.

b. Click the **Apply Changes** button to save the changes for this device.

7. Optionally, click **Enable SSL Mode** if you want to configure secure COM ports.



Windows Drivers Management Console

- DeviceMaster/ICDM-RX
  - DeviceMaster DM-2304
    - Port 01 (COM11)
    - Port 02 (COM212)
    - Port 03 (COM213)
    - Port 04 (COM140)
  - DeviceMaster RTS, 1 Port
    - Port 01 (COM106)
  - DeviceMaster RTS, 4 Port
    - Port 01 (COM99)
    - Port 02 (COM500)
    - Port 03 (COM304)
    - Port 04 (COM101)
  - ICDM-RX/TCP-DB9/RJ45-PM
    - Port 01 (COM3)
- RocketPort Infinity/Express

General | Advanced

Network Connection Mode

○ MAC Mode: 00 0D 81 09 09 FE
● IPv4 Mode: 10.8.11.73
○ IPv6 Mode: FE80::20D:81FF:FE09:9FE
☑ Enable SSL Mode

Device Settings

Device Name: ICDM-RX/TCP-DB9/RJ45-PM
User-Friendly Device Name: ICDM-RX/TCP-DB9/RJ45-PM
Keep Alive Timeout (seconds): 120 (Default: 120)
TCP Timeout Multiplier: 1 (Default: 1)
Scan Rate (ms): 10 (Default: 10)
Verbose Event Log □ (Troubleshooting Only)

Windows Drivers Management Console version 6.04
Copyright © Pepperl+Fuchs. All rights reserved.

Note: *The ICDM-RX/TCP-16RJ45/2RJ45-PM must be configured using* ***IP Mode*** *(IPv4 or IPv6) before you can* ***Enable SSL Mode****.*

If **SSL Mode** is enabled, TCP connections that carry data to/from the serial ports are encrypted using SSL or TLS security protocols. This includes the following:

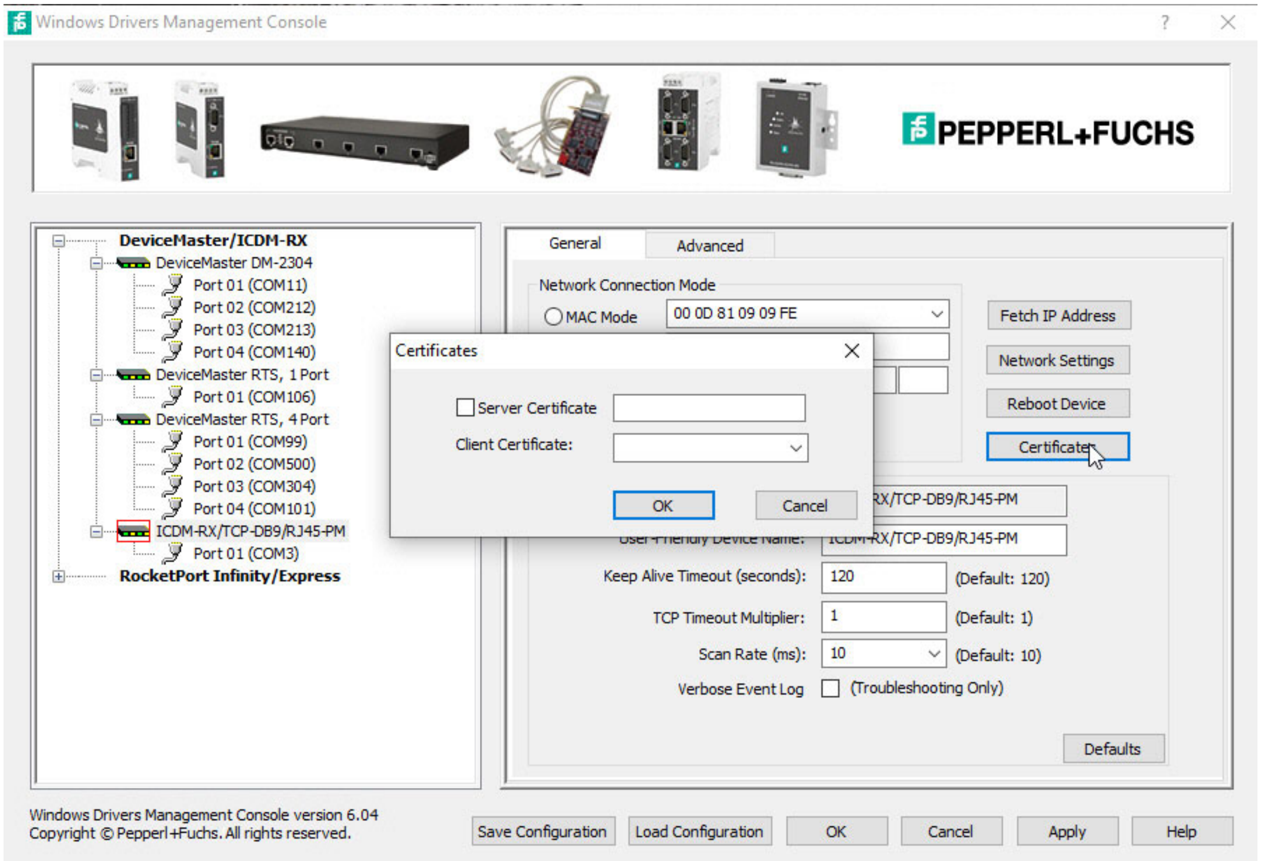
- TCP connections to the per-serial-port TCP ports (default is 8000, 8001, 8002, ...) are encrypted using SSL/TLS.
- TCP connections to TCP port 4606 on which the ICDM-RX/TCP-16RJ45/2RJ45-PM implements the Pepperl+Fuchs proprietary serial driver protocol are encrypted using SSL/TLS.
- Since SSL/TLS can not be used for either UDP data streams or for the Pepperl+Fuchs proprietary MAC mode Ethernet driver protocol, both UDP and MAC mode serial data transport features are disabled.

In addition to encrypting the data streams, it is possible to configure the ICDM-RX/TCP-16RJ45/2RJ45-PM so that only authorized client applications can connect using SSL/TLS.

For this option to function, you must also **Enable Secure Data Mode** in the NS-Link web page.

Note: *See the help system if you need additional information on SSL and the corresponding options.*

8. If you are using a server certificate, click the **Certificates** button.
   a. Click the **Server Certificate** check box if you want to enter a **Server Certificate**.
   b. Enter the name in the **Server Certificate** text box.



DeviceMaster/ICDM-RX
- DeviceMaster DM-2304
  - Port 01 (COM11)
  - Port 02 (COM212)
  - Port 03 (COM213)
  - Port 04 (COM140)
- DeviceMaster RTS, 1 Port
  - Port 01 (COM106)
- DeviceMaster RTS, 4 Port
  - Port 01 (COM99)
  - Port 02 (COM500)
  - Port 03 (COM304)
  - Port 04 (COM101)
- ICDM-RX/TCP-DB9/RJ45-PM
  - Port 01 (COM3)

RocketPort Infinity/Express

Network Connection Mode

○ MAC Mode 00 0D 81 09 09 FE

Certificates

□ Server Certificate

Client Certificate:

RX/TCP-DB9/RJ45-PM

User-Friendly Device Name: ICDM-RX/TCP-DB9/RJ45-PM

Keep Alive Timeout (seconds): 120 (Default: 120)

TCP Timeout Multiplier: 1 (Default: 1)

Scan Rate (ms): 10 (Default: 10)

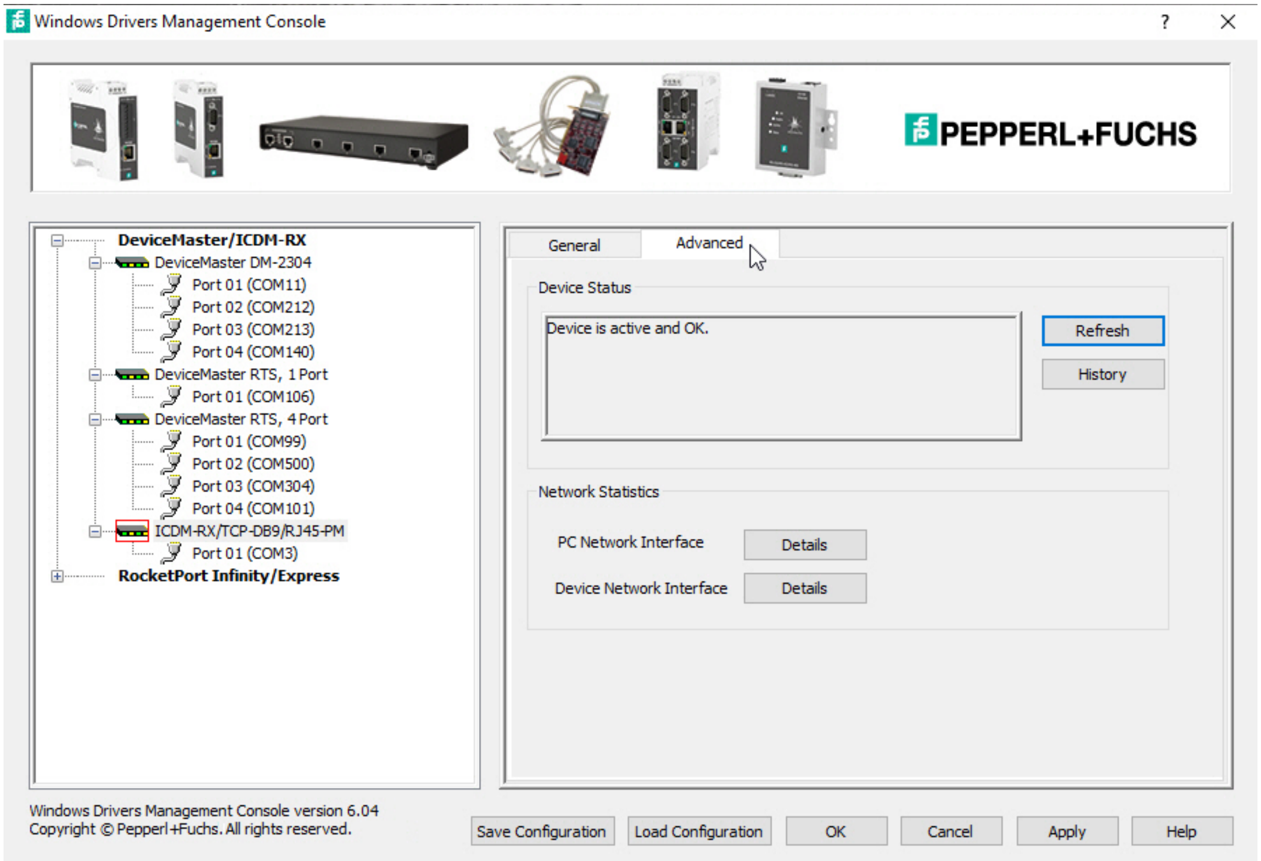
Verbose Event Log □ (Troubleshooting Only)

Windows Drivers Management Console version 6.04
Copyright © Pepperl+Fuchs. All rights reserved.

   c. If you are using a client certificate, click the drop list and browse to the appropriate client certificate file.
   d. Click the **Ok** button to close the *Certificates* pop up window.
9. Configure the remainder of the device properties:
   a. If desired, change the **User-Friendly Device Name**.
   b. Optionally, set a different **Keep Alive Timeout** period. You can set the amount of time in seconds that this ICDM-RX/TCP-16RJ45/2RJ45-PM waits until it closes this connection and frees all the ports associated with it.
   c. Optionally, set the **TCP Timeout Multiplier** value.
   d. Optionally, click a different **Scan Rate (ms)**.
   e. Optionally, click **Verbose Event Log** if you want to log additional ICDM-RX/TCP-16RJ45/2RJ45-PM information into the event log.
   f. After making your changes, click **Apply** if you have additional configuration procedures or click **Ok** if you have completed configuring your ICDM-RX/TCP-16RJ45/2RJ45-PM.

Note: *You can refer to the help system if you need information about any of the options or features.*

10. Optionally, you can click the **Advanced** tab and verify that the *Device Status* message indicates that the ICDM-RX/TCP-16RJ45/2RJ45-PM is active and *Ok*.



Device is active and OK.

Windows Drivers Management Console version 6.04
Copyright © Pepperl+Fuchs. All rights reserved.

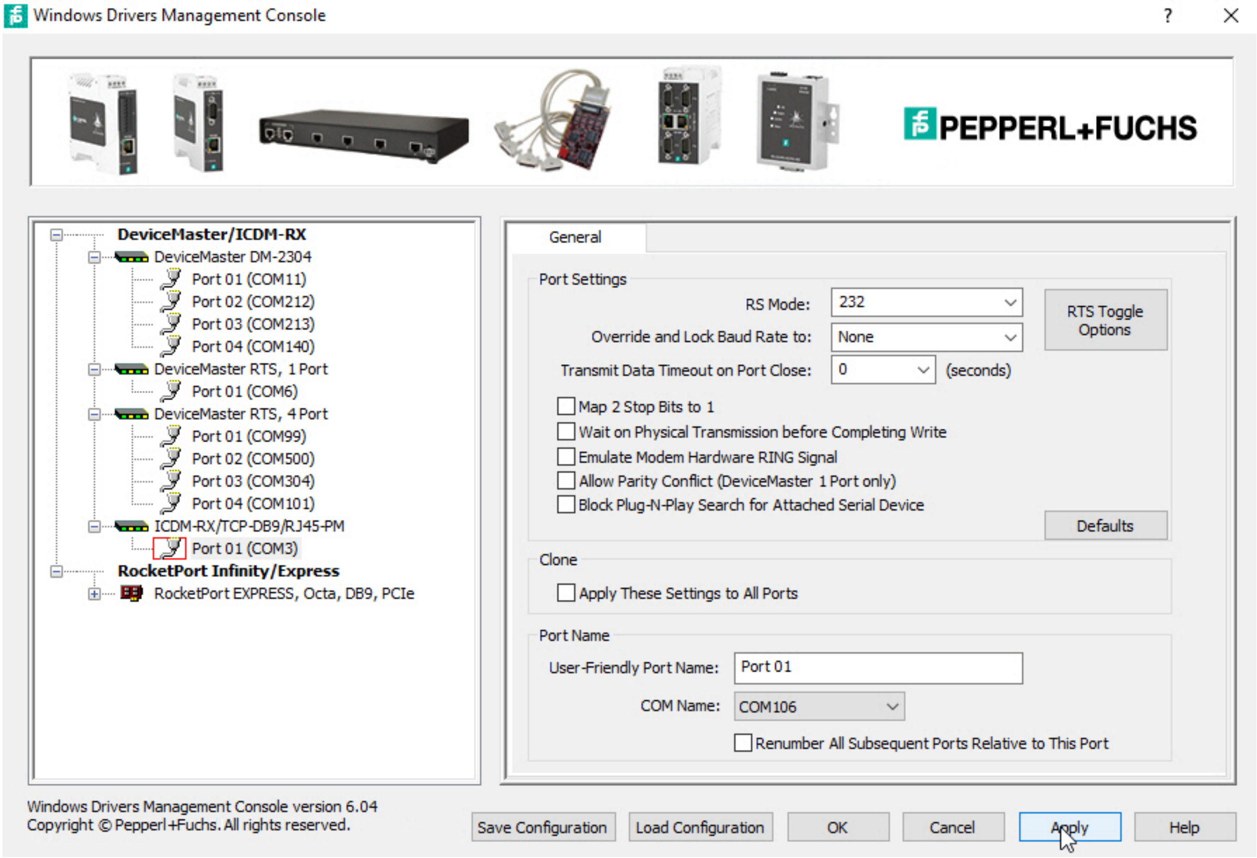
Note: *If you enabled SSL Mode, the status will not be active and Ok until you Enable Secure Data Mode in the web interface using the Network | Security page.*

11. Go to the next subsection to configure COM port properties.

4.5. Configuring COM Port Properties for Windows

The following is a COM port properties configuration overview. Use the NS-Link **Help** system for detailed configuration information.

1. Highlight the first port you want to configure.



Windows Drivers Management Console

- DeviceMaster/ICDM-RX
  - DeviceMaster DM-2304
    - Port 01 (COM11)
    - Port 02 (COM212)
    - Port 03 (COM213)
    - Port 04 (COM140)
  - DeviceMaster RTS, 1 Port
    - Port 01 (COM6)
  - DeviceMaster RTS, 4 Port
    - Port 01 (COM99)
    - Port 02 (COM500)
    - Port 03 (COM304)
    - Port 04 (COM101)
  - ICDM-RX/TCP-DB9/RJ45-PM
    - Port 01 (COM3)
- RocketPort Infinity/Express
  - RocketPort EXPRESS, Octa, DB9, PCIe

General

Port Settings

RS Mode: 232

Override and Lock Baud Rate to: None

Transmit Data Timeout on Port Close: 0 (seconds)

□ Map 2 Stop Bits to 1
□ Wait on Physical Transmission before Completing Write
□ Emulate Modem Hardware RING Signal
□ Allow Parity Conflict (DeviceMaster 1 Port only)
□ Block Plug-N-Play Search for Attached Serial Device

Clone

□ Apply These Settings to All Ports

Port Name

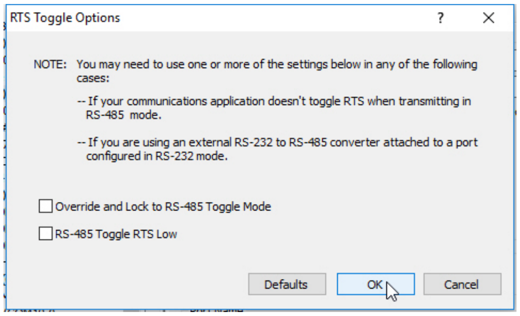
User-Friendly Port Name: Port 01

COM Name: COM106

□ Renumber All Subsequent Ports Relative to This Port

Windows Drivers Management Console version 6.04
Copyright © Pepperl+Fuchs. All rights reserved.

2. Complete the screen appropriately for the serial device that you plan on connecting to the port and click the **Ok** button.
   a. Select the appropriate communications mode.
   b. Enable the features that you want to use.
   c. Optionally, click the **RTS Toggle Options** button:
      - If your communications application does not toggle RTS when transmitting in RS-485 mode.
      - If you are using an external RS-232 to RS-485 converter, which is attached to a port that is configured for RS-232.
   d. Click the appropriate options for your environment.
   e. Click **OK** to save the changes and return to the port **General** tab.



RTS Toggle Options

NOTE: You may need to use one or more of the settings below in any of the following cases:

-- If your communications application doesn't toggle RTS when transmitting in RS-485 mode.

-- If you are using an external RS-232 to RS-485 converter attached to a port configured in RS-232 mode.

□ Override and Lock to RS-485 Toggle Mode
□ RS-485 Toggle RTS Low

3. If desired, click the **Clone** check box to set all of the ports on this ICDM-RX/TCP-16RJ45/2RJ45-PM to these characteristics.
4. Optionally, change the **User-Friendly Port Name**.

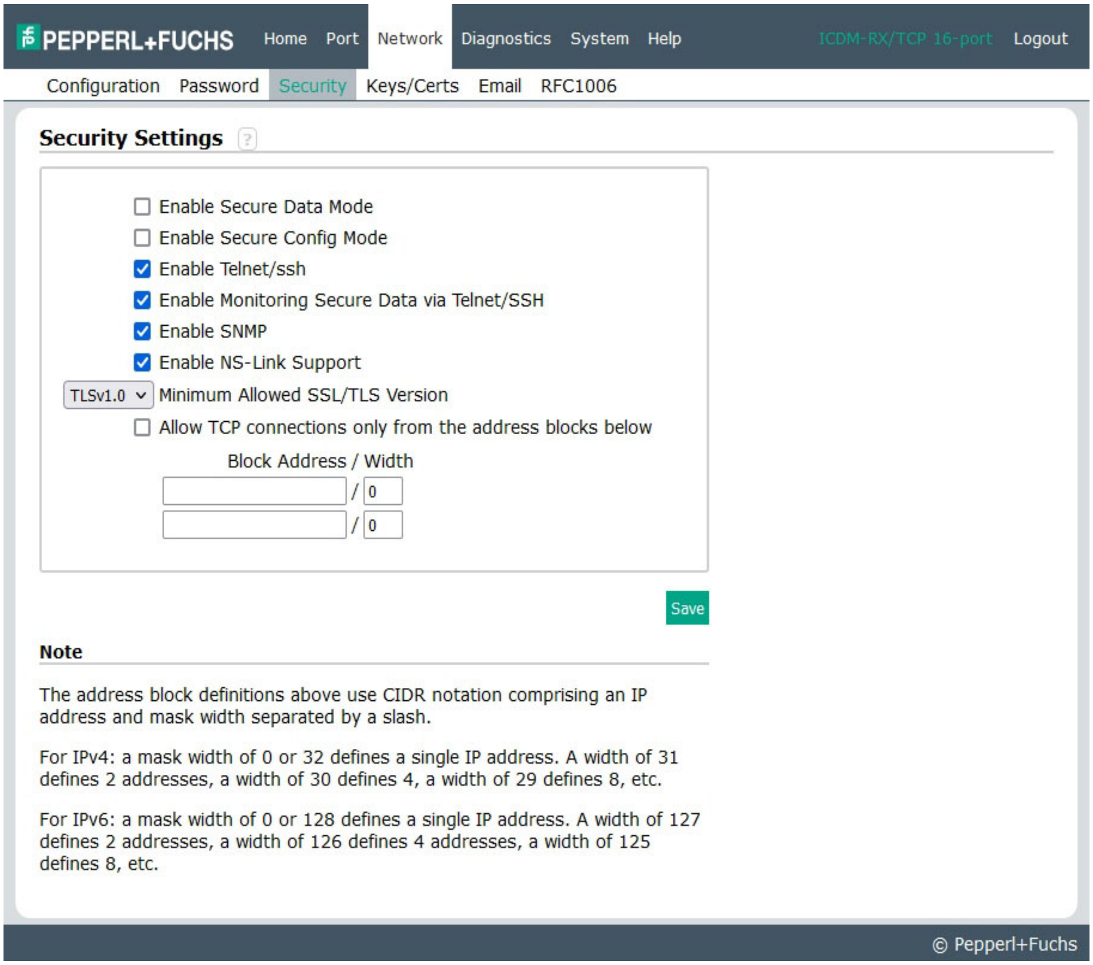
5. If desired, select a different **COM Name** (COM port number). The drop-down list displays (in use) next to COM port numbers that are already in use in this system. Do not duplicate COM port numbers as this will cause the ports to not function.
6. Click **Apply** to save these changes.

   Note: *If you selected RS-422 mode, make sure that there is not a device attached to the port and click* **Ok***.*
7. Highlight the next port that you want to configure and perform Steps 1 through 6.
8. Refer to *Connecting Serial Devices* on Page 76 to attach your serial device.
9. Optionally, you may need to configure one or more ports for socket mode (*Socket Port Configuration* on Page 30).

4.6. Enabling Secure Data Mode

In addition to enabling **SSL Mode** in the driver, you must **Enable Secure Data Mode** in the NS-Link web page. Use the following procedure to implement the **Enable Secure Data Mode** option.

1. Access the NS-Link web page using one of these methods:
    - Open your web browser, enter the IP address, and press **Enter**.
    - Right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM in PortVision DX and click **Webpage**.
2. Click **Network | Security**.
3. Click **Enable Secure Data Mode** and **Save**.



Security Settings

☐ Enable Secure Data Mode
☐ Enable Secure Config Mode
☑ Enable Telnet/ssh
☑ Enable Monitoring Secure Data via Telnet/SSH
☑ Enable SNMP
☑ Enable NS-Link Support
TLSv1.0 Minimum Allowed SSL/TLS Version
☐ Allow TCP connections only from the address blocks below

Block Address / Width
/ 0
/ 0

Note

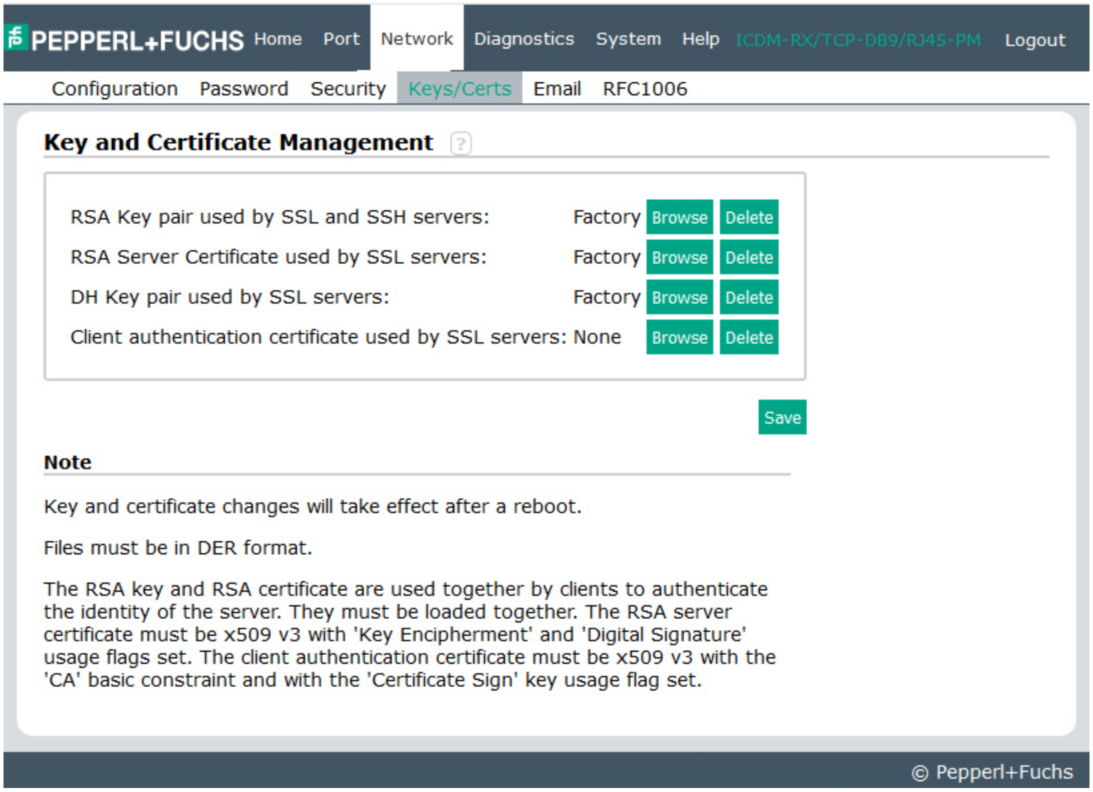
The address block definitions above use CIDR notation comprising an IP address and mask width separated by a slash.

For IPv4: a mask width of 0 or 32 defines a single IP address. A width of 31 defines 2 addresses, a width of 30 defines 4, a width of 29 defines 8, etc.

For IPv6: a mask width of 0 or 128 defines a single IP address. A width of 127 defines 2 addresses, a width of 126 defines 4 addresses, a width of 125 defines 8, etc.

4. Click **Keys/Certs** to configure your security key and certificate.

5. Click the appropriate **Browse** button to locate your key or certificate and click **Save** when you are done



Key and Certificate Management

RSA Key pair used by SSL and SSH servers: Factory

RSA Server Certificate used by SSL servers: Factory

DH Key pair used by SSL servers: Factory

Client authentication certificate used by SSL servers: None

Note

Key and certificate changes will take effect after a reboot.

Files must be in DER format.

The RSA key and RSA certificate are used together by clients to authenticate the identity of the server. They must be loaded together. The RSA server certificate must be x509 v3 with 'Key Encipherment' and 'Digital Signature' usage flags set. The client authentication certificate must be x509 v3 with the 'CA' basic constraint and with the 'Certificate Sign' key usage flag set.

Click the **Help** button if you need information about key and certificate management.

5. Socket Port Configuration

This section provides an overview of SocketServer and provides basic operating procedures. SocketServer and ICDM-RX/TCP-16RJ45/2RJ45-PM security are discussed in detail in *ICDM-RX/TCP-16RJ45/2RJ45-PM Security* on Page 36.

Note: *Technical Supports recommends that you update to the latest version of SocketServer before installing an NS-Link device driver or configuring socket ports.*

5.1. SocketServer Overview

SocketServer is the name of the TCP/IP socket web page that is integrated in the firmware that comes pre-installed on your ICDM-RX/TCP-16RJ45/2RJ45-PM. When you install an NS-Link device driver, an NS-Link version of SocketServer loads on the ICDM-RX/TCP-16RJ45/2RJ45-PM.

The SocketServer home page (*Server Info*) provides basic information about the ICDM-RX/TCP-16RJ45/2RJ45-PM including whether it is functioning in socket mode (SocketServer) or in NS-Link (driver). See *SocketServer Architecture* on Page 31 for more information about socket port support.

The following menus are available in the web interface:

- **Port**, which includes the following pages:
  - **Port Overview** of all of the serial port settings
  - **Port Configuration** for each port that includes Serial, TCP connection, and UDP connection configuration capabilities
- **Network**, which includes the following pages:
  - **Configuration** for general, IPv4 and IPv6 settings (after initial configuration)
  - **Password** to set a device password
  - **Security**, which is discussed in detail starting on Page 36
  - **Keys/Certs** to manage security keys and certificates
  - **Email** for notification services
  - **RFC1006** (ISO over TCP)
- **Diagnostics**, which includes:
  - **System Log**
  - **Port Monitor**
- **System**, which includes:
  - **Update Firmware**
  - **Configuration File**
  - **System Snapshot**
  - **Restore Defaults**
  - **Reboot**

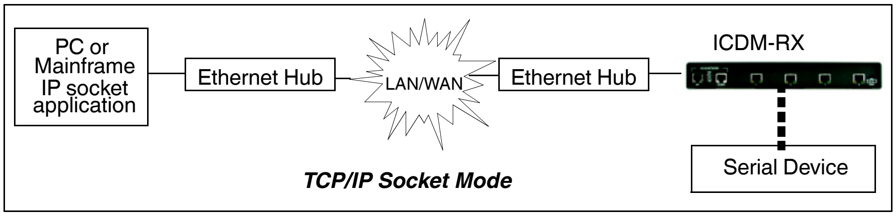
Note: *For socket service configuration procedures or information, see the web page Help system.*

5.1.1. Web Page Help System

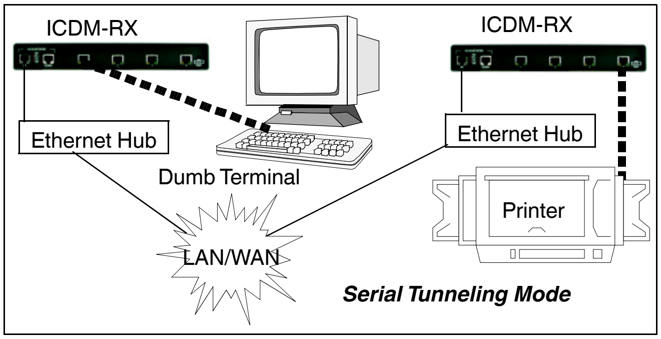
The web page Help system contains detailed information and configuration procedures for each mode discussed in *SocketServer Architecture* on Page 31.

5.1.2. SocketServer Architecture

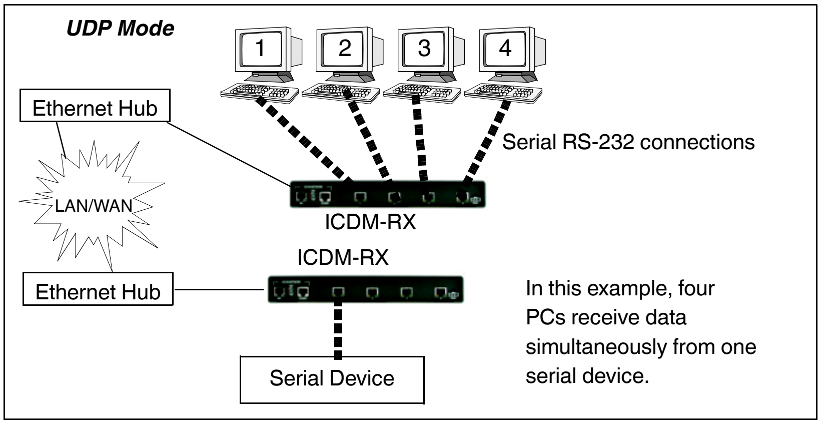
TCP/IP socket mode operation is used to connect serial devices with an application that supports TCP/IP socket communications addressing.



Serial tunneling mode is used to establish a socket connection between two ICDM-RX/TCP-16RJ45/2RJ45-PMs through an Ethernet network.



UDP mode is designed for applications that need faster data transmission, or that make use of UDP's broadcast capabilities. UDP differs from TCP in that a UDP transmission does not first require a connection to be opened before sending data and the receiving device does not issue acknowledgments to the sender.


UDP Mode
1
2
3
4
Ethernet Hub
Serial RS-232 connections
LAN/WAN
ICDM-RX
ICDM-RX
Ethernet Hub
Serial Device
In this example, four PCs receive data simultaneously from one serial device.

5.2. Accessing Socket Configuration

There are two ways to access the socket configuration pages. Use the method that fits your environment best.

- *Web Browser*
- *PortVision DX*

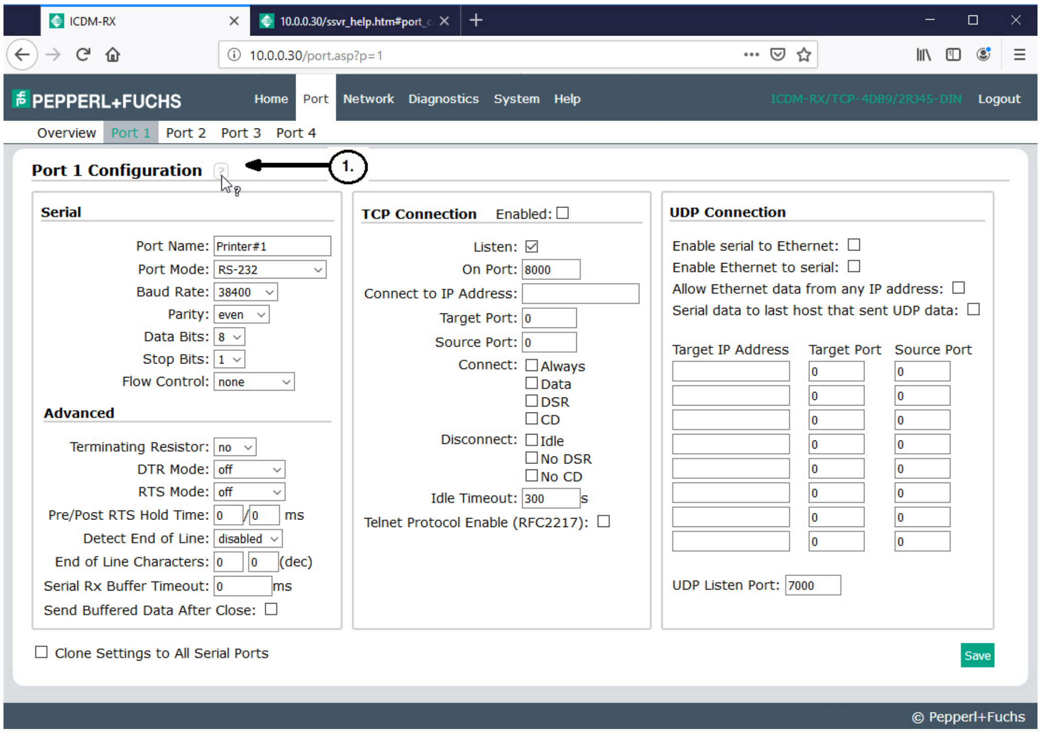
5.2.1. Web Browser

To access the socket configuration web interface for the ICDM-RX/TCP-16RJ45/2RJ45-PM, follow this procedure.

1. Start your web browser.
2. Enter the IP address of the ICDM-RX/TCP-16RJ45/2RJ45-PM in the URL field.

   Note: *If you do not know the IP address, you can view and highlight the IP address in PortVision DX and click the* **Webpage** *button.*
3. If necessary, enter **admin** as the *username*, your password, and then click the **Login** button.
4. Click the **Port** menu.
5. Click the port number that you want to configure socket port settings (serial, TCP connection configuration, and UDP connection configuration).

Note: *Refer to the web page Help system, if you need information about configuring sockets or serial tunneling, which contains detailed configuration procedures and descriptions for all fields.*



Port 1 Configuration

Serial

Port Name: Printer#1
Port Mode: RS-232
Baud Rate: 38400
Parity: even
Data Bits: 8
Stop Bits: 1
Flow Control: none

Advanced

Terminating Resistor: no
DTR Mode: off
RTS Mode: off
Pre/Post RTS Hold Time: 0 / 0 ms
Detect End of Line: disabled
End of Line Characters: 0 0 (dec)
Serial Rx Buffer Timeout: 0 ms
Send Buffered Data After Close: □

TCP Connection Enabled: □

Listen: ☑
On Port: 8000
Connect to IP Address:
Target Port: 0
Source Port: 0
Connect: □ Always □ Data □ DSR □ CD
Disconnect: □ Idle □ No DSR □ No CD
Idle Timeout: 300 s
Telnet Protocol Enable (RFC2217): □

UDP Connection

Enable serial to Ethernet: □
Enable Ethernet to serial: □
Allow Ethernet data from any IP address: □
Serial data to last host that sent UDP data: □

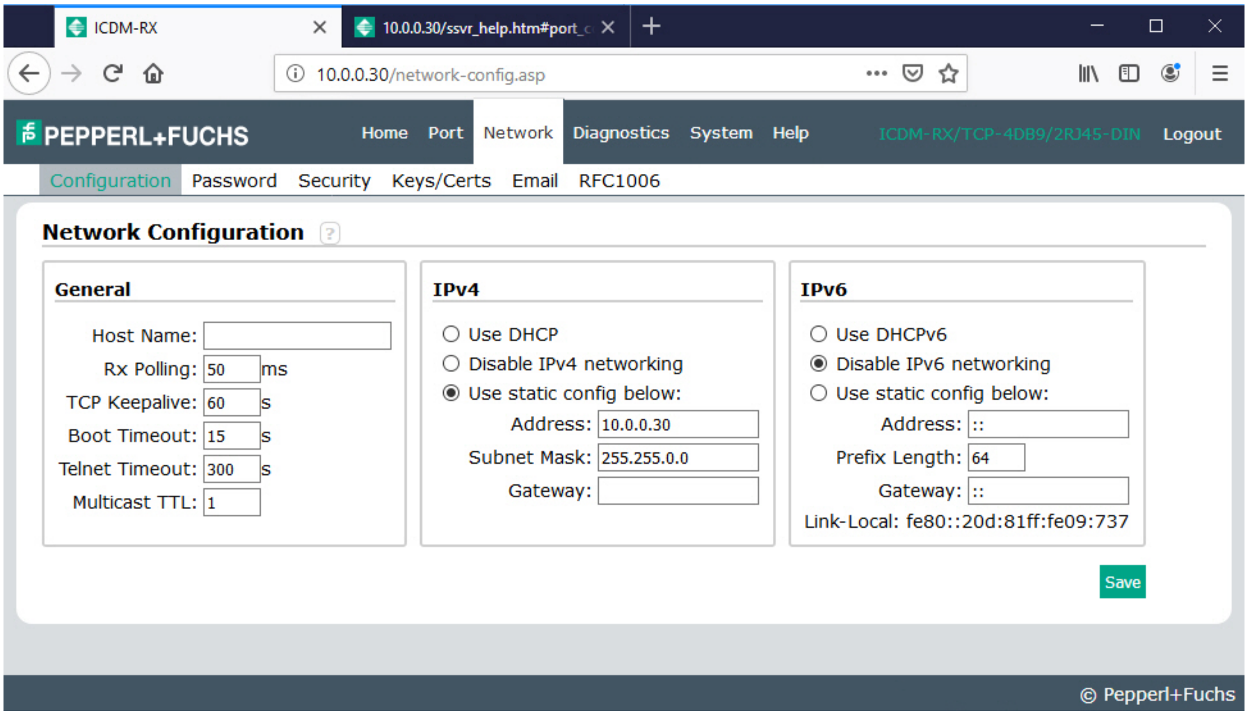
Target IP Address	Target Port	Source Port
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0

UDP Listen Port: 7000

□ Clone Settings to All Serial Ports

2. After changing the appropriate settings for your environment, click **Save**.
3. Click the **Network** tab to access the following pages if you need to configure additional settings:
   - **Configuration** page to change the network settings.
   - **Password** page to configure a password for the ICDM-RX/TCP-16RJ45/2RJ45-PM.

- **Security** page to enable ICDM-RX/TCP-16RJ45/2RJ45-PM security.
- **Keys/Certs** page to configure security certificates and keys.
- **Email** page to configure email notification services.
- **RFC1006** page to configure RFC1006 settings.



Network Configuration

General

Host Name:

Rx Polling: 50 ms

TCP Keepalive: 60 s

Boot Timeout: 15 s

Telnet Timeout: 300 s

Multicast TTL: 1

IPv4

○ Use DHCP

○ Disable IPv4 networking

● Use static config below:

Address: 10.0.0.30

Subnet Mask: 255.255.0.0

Gateway:

IPv6

○ Use DHCPv6

● Disable IPv6 networking

○ Use static config below:

Address: ::

Prefix Length: 64

Gateway: ::

Link-Local: fe80::20d:81ff:fe09:737

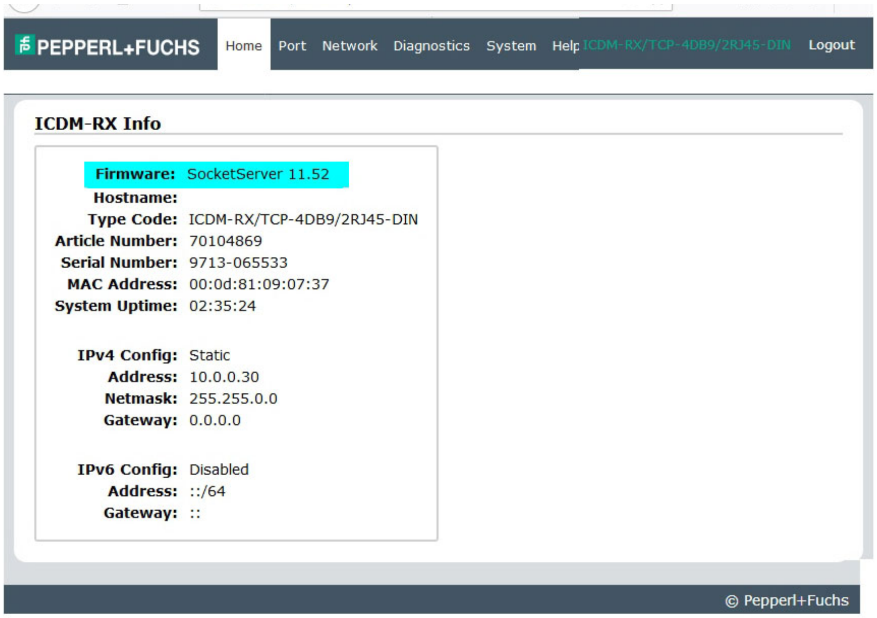
5.2.2. PortVision DX

There are several ways to access the socket configuration page for the ICDM-RX/TCP-16RJ45/2RJ45-PM using PortVision DX.

1. If necessary, start PortVision DX, right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM that you want to configure, and click **Webpage**.
2. Follow Steps 3 through 3 from the previous procedure above (*Web Browser*).

5.3. SocketServer Versions

The *SocketServer Overview* discusses the that the default SocketServer web page is the same as the NS-Link web page. If the NS-Link driver is not running (not installed or disabled), SocketServer loads when you open a web browser session.



ICDM-RX Info

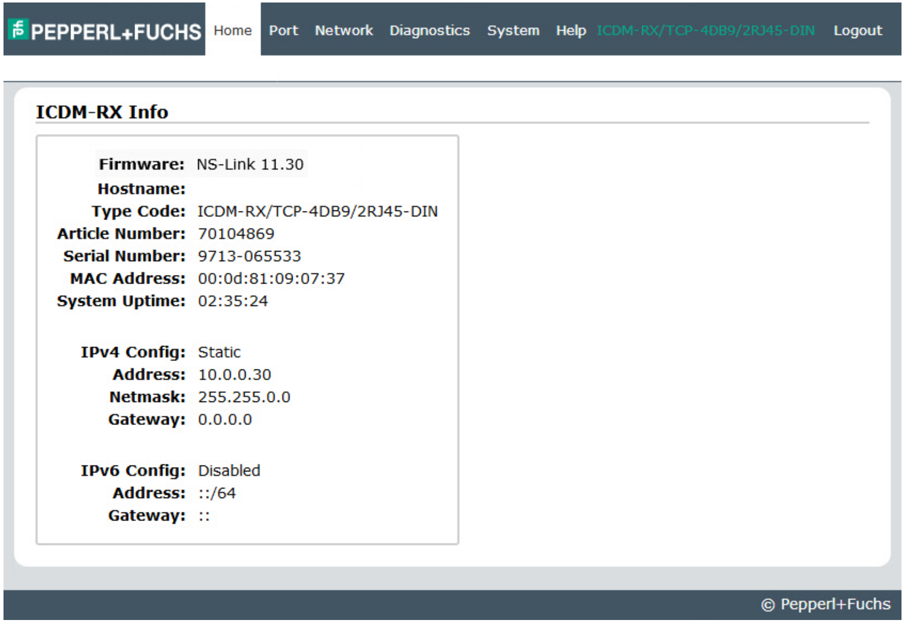
Firmware: SocketServer 11.52
Hostname:
Type Code: ICDM-RX/TCP-4DB9/2RJ45-DIN
Article Number: 70104869
Serial Number: 9713-065533
MAC Address: 00:0d:81:09:07:37
System Uptime: 02:35:24

IPv4 Config: Static
Address: 10.0.0.30
Netmask: 255.255.0.0
Gateway: 0.0.0.0

IPv6 Config: Disabled
Address: ::/64
Gateway: ::

Note: *The top illustration shows the web page before an NS-Link device driver installation and the bottom illustration shows the web page after a device driver installation.*

Your SocketServer or NS-Link version may be different than these examples.



ICDM-RX Info

Firmware:	NS-Link 11.30
Hostname:	
Type Code:	ICDM-RX/TCP-4DB9/2RJ45-DIN
Article Number:	70104869
Serial Number:	9713-065533
MAC Address:	00:0d:81:09:07:37
System Uptime:	02:35:24
IPv4 Config:	Static
Address:	10.0.0.30
Netmask:	255.255.0.0
Gateway:	0.0.0.0
IPv6 Config:	Disabled
Address:	::/64
Gateway:	::

6. ICDM-RX/TCP-16RJ45/2RJ45-PM Security

This subsection provides a basic understanding of the ICDM-RX/TCP-16RJ45/2RJ45-PM security options, and the repercussions of setting these options. See *Removing ICDM-RX/TCP-16RJ45/2RJ45-PM Security Features* on Page 121 if you need to reset ICDM-RX/TCP-16RJ45/2RJ45-PM security options. See *Restoring Defaults* on Page 84 if you want to return the ICDM-RX/TCP-16RJ45/2RJ45-PM settings to their default values.

6.1. Understanding Security Methods and Terminology

The following table provides background information and definitions.

Term or Issue Explanation	
CA (Client Authentication certificate) †	If configured with a CA certificate, the ICDM-RX/TCP-16RJ45/2RJ45-PM requires all SSL/TLS clients to present an RSA identity certificate that has been signed by the configured CA certificate. As shipped, the ICDM-RX/TCP-16RJ45/2RJ45-PM is not configured with a CA certificate and all SSL/TLS clients are allowed. This uploaded CA certificate that is used to validate a client's identity is sometimes referred to as a *trusted root certificate*, a *trusted authority certificate*, or a *trusted CA certificate*. This CA certificate might be that of a trusted commercial certificate authority or it may be a privately generated certificate that an organization creates internally to provide a mechanism to control access to resources that are protected by the SSL/TLS protocols. See *Key and Certificate Management* on Page 53 for more information. This section does not discuss the creation of CA Certificates.
Client Authentication	A process using paired keys and identity certificates to prevent unauthorized access to the ICDM-RX/TCP-16RJ45/2RJ45-PM. Client authentication is discussed in *Client Authentication* on Page 44 and *Changing Keys and Certificates* on Page 56.
DH Key Pair Used by SSL Servers †	This is a private/public key pair that is used by some cipher suites to encrypt the SSL/TLS handshaking messages. Possession of the private portion of the key pair allows an eavesdropper to decrypt traffic on SSL/TLS connections that use DH encryption during handshaking. The DH (Diffie-Hellman) key exchange, also called exponential key exchange, is a method of digital encryption that uses numbers raised to specific powers to produce decryption keys on the basis of components that are never directly transmitted, making the task of a would-be code breaker mathematically overwhelming. The most serious limitation of Diffie-Hellman (DH key) in its basic or *pure* form is the lack of authentication. Communications using Diffie-Hellman all by itself are vulnerable to man in the middle attacks. Ideally, Diffie-Hellman should be used in conjunction with a recognized authentication method such as digital signatures to verify the identities of the users over the public communications medium. See *Certificates and Keys* on Page 44 and *Key and Certificate Management* on Page 53 for more information.
† *All ICDM-RX/TCP-16RJ45/2RJ45-PM units are shipped from the factory with identical configurations. They all have the identical, self-signed, Pepperl+Fuchs Server RSA Certificates, Server RSA Keys, Server DH Keys, and no Client Authentication Certificates. For maximum data and access security, you should configure all ICDM-RX/TCP-16RJ45/2RJ45-PM units with custom certificates and keys.*	

Term or Issue Explanation (Continued)	
Digital Certificate	A digital certificate is an electronic *credit card* that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys. See *Key and Certificate Management* on Page 53 for more information.
PKI (public key infrastructure)	A public key infrastructure (PKI) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on. The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. (The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography.) A public key infrastructure consists of: • A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key • A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor • One or more directories where the certificates (with their public keys) are held • A certificate management system For more information, see *SSL Authentication* on Page 43, *SSL Performance* on Page 46, *SSL Cipher Suites* on Page 46, and *ICDM-RX/TCP-16RJ45/2RJ45-PM Supported Cipher Suites* on Page 47.

Term or Issue Explanation (Continued)	
RSA Key Pair†	This is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption. RSA is widely used in electronic commerce protocols, and is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations. The system includes a communications channel coupled to at least one terminal having an encoding device, and to at least one terminal having a decoding device. • Public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures. • Private Key - One half of the *key pair* used in conjunction with a public key - Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet. - The private key is used to decrypt text that has been encrypted with the public key. Thus, if *User A* sends *User B* a message, *User A* can find out *User B's* public key (but not *User B's* private key) from a central administrator and encrypt a message to *User B* using *User B's* public key. When *User B* receives it, *User B* decrypts it with *User B's* private key. In addition to encrypting messages (which ensures privacy), *User B* can authenticate *User B* to *User A* (so that *User A* knows that it is really *User B* who sent the message) by using *User B's* private key to encrypt a digital certificate. See *Key and Certificate Management* on Page 53 for more information.
SSH (Secure Shell)	Secure Shell (SSH) allows data to be exchanged using a secure channel between two networked devices. Replaces telnet which has no security. SSH requires password authentication – even if the password is empty. See *SSH Server* on Page 43 for more information.
SSL (Secure Sockets Layer)	The Secure Sockets Layer (SSL) is the predecessor of (TLS) Transport Layer Security. SSL is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. See Pages 43 through 47 for detailed information about SSL. ***Note:*** *Two slightly different SSL protocols are supported by the ICDM-RX/TCP-16RJ45/2RJ45-PM: SSLv3 and TLSv1.*
TLS (Transport Layer Security)	Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL). TLS and SSL are not interoperable. The TLS protocol does contain a mechanism that allows TLS implementation to back down to SSL 3.0.
Secure Data Mode	TCP connections that carry data to/from the ICDM-RX/TCP-16RJ45/2RJ45-PM serial ports are encrypted using SSL or TLS security protocols. See *Secure Data and Secure Config Modes* on Page 41 and *Configure/Enable Security Features Overview* on Page 48 for more information.

Term or Issue Explanation (Continued)	
Secure Config Mode	Unencrypted access to administrative and diagnostic functions are disabled. See *Secure Data and Secure Config Modes* on Page 41 and *Configure/Enable Security Features Overview* on Page 48 for more information.
Secure Monitor Data Mode via Telnet	Allows monitoring of a single serial port on the ICDM-RX/TCP-16RJ45/2RJ45-PM while the port is configured for **Secure Data Mode**. For more information see, the **Enable Monitoring Secure Data via Telnet** option on Page 50.
Man in the Middle attack	A man in the middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other. The attack gets its name from the ball game where two people try to throw a ball directly to each other while one person in between them attempts to catch it. In a man in the middle attack, the intruder uses a program that appears to be the server to the client and appears to be the client to the server. The attack may be used simply to gain access to the message, or enable the attacker to modify the message before retransmitting it.
How Public and Private Key Cryptography Works	In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA). The private key is given only to the requesting party and the public key is made publicly available (as part of a digital certificate) in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. You use the private key to decrypt text that has been encrypted with your public key by someone else (who can find out what your public key is from a public directory). Thus, if *User A* sends *User B* a message, *User A* can find out *User B's* public key (but not *User B's* private key) from a central administrator and encrypt a message to *User B* using *User B's* public key. When *User B* receives it, *User B* decrypts it with *User B's* private key. In addition to encrypting messages (which ensures privacy), *User B* can authenticate *User B* to *User A* (so *User A* knows that it is really *User B* who sent the message) by using *User B's* private key to encrypt a digital certificate. When *User A* receives it, *User A* can use *User B's* public key to decrypt it.
Who Provides the Infrastructure?	A number of products are offered that enable a company or group of companies to implement a PKI. The acceleration of e-commerce and business-to-business commerce over the Internet has increased the demand for PKI solutions. Related ideas are the virtual private network (VPN) and the IP Security (IPsec) standard. Among PKI leaders are: • RSA, which has developed the main algorithms used by PKI vendors. • Verisign, which acts as a certificate authority and sells software that allows a company to create its own certificate authorities. • GTE CyberTrust, which provides a PKI implementation methodology and consultation service that it plans to vend to other companies for a fixed price. • Xcert, whose Web Sentry product that checks the revocation status of certificates on a server, using the Online Certificate Status Protocol (OCSP). • Netscape, whose Directory Server product is said to support 50 million objects and process 5,000 queries a second; Secure E-Commerce, which allows a company or extranet manager to manage digital certificates; and Meta-Directory, which can connect all corporate directories into a single directory for security management.

Term or Issue Explanation (Continued)
The following topic references are from: http://searchsecurity.techtarget.com/ • PKI (public key infrastructure) • How Public/Private Key Cryptography Works • Who Provides the Infrastructure • Digital Certificate • DH Key • Man in the Middle attack The RSA Key pair topic reference is from: http://en.wikipedia.org/wiki/RSA

6.2. TCP and UDP Socket Ports Used by the ICDM-RX/TCP-16RJ45/2RJ45-PM

Following list is all of the logical TCP and UDP socket ports implemented in ICDM-RX/TCP-16RJ45/2RJ45-PMs.

Socket Port Number Descriptions	
22 SSH 23 Telnet	TCP Ports 22 (ssh) and 23 (telnet) are used for administrative and diagnostic purposes and aren't required for normal use and are enabled by default and Port 23 may be disabled.
80 HTTP 443 SSL or HTTPS	TCP Ports 80 (http) and 443 (https) are used by the web server for administration and configuration and are enabled by default and cannot be disabled.
102 RFC1006	TCP Port 102 is used for RFC1006 (ISO over TCP) serial port access. Not used for normal NS-Link SocketServer access. The RFC1006 server can be disabled by setting the server port number to -1 and is enabled by default.
161 SNMP	UDP Port 161 is used by the SNMP agent if SNMP is enabled which is the default.
4606	TCP Port 4606 is required if you want to use the web interface or PortVision DX if you want to update firmware without setting up a TFTP server and this port cannot be disabled.
4607	TCP Port 4607 is only used for diagnostic purposes and is not required for normal operation and this port cannot be disabled. If SocketServer is to be used, then the user may enable usage of TCP or UDP ports for access to the serial ports. These ports are not enabled by default and are also user configurable to different values. Defaults for TCP would begin at 8000 and for UDP would begin at 7000.
TCP 8000 - 8xxx	Incremented per serial port on the ICDM-RX/TCP-16RJ45/2RJ45-PM. For example: An ICDM-RX/TCP-16RJ45/2RJ45-PM 4-port would have Ports 8000 through 8003.
UDP 7000 - 7xxx	Incremented per serial port on the ICDM-RX/TCP-16RJ45/2RJ45-PM. For example: An ICDM-RX/TCP-16RJ45/2RJ45-PM 4-port would have Ports 7000 through 7003.

6.3. ICDM-RX/TCP-16RJ45/2RJ45-PM Security Features

The following subsections provide information about ICDM-RX/TCP-16RJ45/2RJ45-PM security features.

6.3.1. Secure Data and Secure Config Modes

The ICDM-RX/TCP-16RJ45/2RJ45-PM supports Secure Data and Secure Config modes.

Security Mode Information	
Secure Data	SSL encryption for serial port data streams for both NS-Link and SocketServer. **Secure Data mode**: • Requires SSL encryption of TCP connections to SocketServer (Ports 8000, 8001, 8002, and so forth). • Disables UDP access to SocketServer. • Disables RFC1006 (ISO-over-TCP) access to SocketServer. • Disables MAC-mode access to serial ports. MAC mode admin and ID commands are still allowed. • Requires SSL encryption of NS-Link TCP connections (Port 4606). Not directly supported by NS-Link drivers for Windows and Linux. The Linux driver has been tested using stunnel, but manual setup is required. • Requires SSH instead of telnet connection to the diagnostic log (TCP Port 4607). • Two values for http READ and WRITE commands: A2: Enable.
Secure Config	Encrypts/authenticates configuration and administration operations (web server, IP settings, load SW, and so forth.). **Secure Config mode**: • Disables MAC mode admin commands except for ID request†. • Disables TCP/IP admin commands except for ID request†. • Disables telnet console access (Port 23)†. • Disables unencrypted http:// access via Port 80. • Disables e-mail notification and SNMP features. • Two values for http READ and WRITE commands: A3: Enable.
† *Affects both RedBoot and SocketServer/NS-Link applications.*	

6.3.2. Secure Data Mode and Secure Config Mode Comparison

This table provides information that compares **Secure Data** and **Secure Config** modes.

Feature	Secure Data	Secure Config	Secure Data/Secure Config
MAC (admin)	enabled	disabled †	disabled †
MAC (async)	disabled	enabled	disabled
TCP 4606 (admin)	SSL, enabled	clear, disabled †	SSL, disabled †
TCP 4606 (async)	SSL	clear	SSL
UDP	disabled	user-configured	disabled
telnet/RFC2217	user-configured	user-configured	user-configured
RFC1006	disabled	user-configured	disabled
4607 (diag log)	SSH	telnet	SSH
8000 (serial port)	SSL	clear	SSL
console (config)	telnet on Port 23 SSH on Port 22	SSH on Port 22	SSH on Port 22
web	clear on Port 80 SSL on Port 443	SSL on Port 443	SSL on Port 443
SMTP, SNMP	user-configured	disabled	disabled
RedBoot MAC	enabled	disabled †	disabled †
RedBoot 4606	enabled	disabled †	disabled †
RedBoot telnet	user-configured	disabled	disabled

6.3.3. Security Comparison

This table displays addition information about security feature comparisons.

	Weakest					Strongest
	0	1	2	3	3	4
Supported by	None	Password	Authentication	Secure Config	Secure Data	Key & Certificate
RedBoot	yes	yes	yes	no	yes	no
SocketServer	yes	yes	yes	yes	yes	yes
NS-Link Driver/MAC	yes	yes	yes	no	no	no
NS-Link Driver/IP	yes	yes	yes	yes		
Serial Monitoring	yes	yes	yes	no	yes †	no
TCP to Serial Ports	yes	yes	yes	no	no	no
SSH to Serial Ports	no	no	no	yes	yes	yes
UDP to Serial Ports	yes	yes	yes	disabled	disabled	disabled
Telnet/Port23	yes	yes	yes	disabled	yes †	disabled
SSH Telnet/Port 22	yes	yes	yes	yes	yes	yes

		Weakest				Strongest
Telnet Port 4607	yes	yes	yes	disabled	yes	yes
SSH (PuTTY) 4607	no	no	no	yes	disabled	disabled
HTTP (Port 80)	yes	yes	yes	disabled	disabled	disabled
HTTPS (Port 443)	no	no	no	yes	yes	yes
Email	yes	yes	yes	disabled	disabled	disabled
SNMP	yes	yes	yes	disabled	disabled	disabled
RFC1006	yes	yes	yes	disabled	disabled	disabled

† *Enable Monitoring Secure Data via Telnet must be enabled. SSH does not support port monitoring. You can set the* ***securemon enable*** *option.*

admin commands are disabled except for read-only ID command required by NS-Link to identify the device.

The intention is to allow NS-Link to operate through an SSL connection to Port 4606 while is in **Secure Data Mode**, and to allow NS-Link to operate through a MAC connection with **Secure Config Mode** enabled and **Secure Data Mode** disabled.

6.3.4. SSH Server

The ICDM-RX/TCP-16RJ45/2RJ45-PM SSH server has the following characteristics:

- Requires password authentication – even if the password is empty.
- Enabled/disabled along with telnet access independently of **Secure Data** and **Secure Config** modes.
- The ICDM-RX/TCP-16RJ45/2RJ45-PM uses third-party MatrixSSH library from PeerSec Networks: http://www.peersec.com/.

6.3.5. SSL Overview

ICDM-RX/TCP-16RJ45/2RJ45-PM SSL provides the following features:

- Provides both encryption and authentication.
  - Encryption prevents a third-party eavesdropper from viewing data that is being transferred.
  - Authentication allows both the client (that is, web browser) and server (that is. ICDM-RX/TCP-16RJ45/2RJ45-PM) to ensure that only desired parties are allowed to establish connections. This prevents both unauthorized access and man-in-the-middle attacks on the communications channel.
- Several slightly different SSL protocols are supported by the ICDM-RX/TCP-16RJ45/2RJ45-PM, SSLv3, TLSv1.0, TLS1.1, and TLS1.2.
- The ICDM-RX/TCP-16RJ45/2RJ45-PM uses third-party MatrixSSL library from PeerSec Networks: http://www.peersec.com/matrixssl.html.

6.3.6. SSL Authentication

ICDM-RX/TCP-16RJ45/2RJ45-PM SSL authentication has the following features:

- Authentication means being able to verify the identity of the party at the other end of a communications channel. A username/password is a common example of authentication.
- SSL/TLS protocols allow authentication using either RSA certificates or DSS certificates. ICDM-RX/TCP-16RJ45/2RJ45-PM supports only RSA certificates.

- Each party (client and server) can present an ID certificate to the other.
- Each ID certificate is signed by another *authority* certificate or key.
- Each party can then verify the validity of the other's ID certificate by verifying that it was signed by a trusted authority. This verification requires that each party have access to the certificate/key that was used to sign the other party's ID certificate.

6.3.6.1. Server Authentication

Server Authentication is the mechanism by which the ICDM-RX/TCP-16RJ45/2RJ45-PM proves its identity.

- The ICDM-RX/TCP-16RJ45/2RJ45-PM (generally an SSL server) can be configured by uploading an ID certificate that is to be presented to clients when they connect to the ICDM-RX/TCP-16RJ45/2RJ45-PM.
- The private key used to sign the certificate must also be uploaded to the ICDM-RX/TCP-16RJ45/2RJ45-PM.

  Note: *Possession of that private key will allow eavesdroppers to decrypt all traffic to and from the ICDM-RX/TCP-16RJ45/2RJ45-PM.*
- The corresponding public key can be used to verify the ID certificate but not to decrypt traffic.
- All ICDM-RX/TCP-16RJ45/2RJ45-PM are shipped from the factory with identical self-signed ID certificates and private keys. This means that somebody could (with a little effort) extract the factory default private key from the ICDM-RX/TCP-16RJ45/2RJ45-PM firmware and use that private key to eavesdrop on traffic to/ from any other ICDM-RX/TCP-16RJ45/2RJ45-PM that is being used with the default private key.
- The public/private key pairs and the ID certificates can be generated using **openssl** command-line tools.
- If the server authentication certificate in the ICDM-RX/TCP-16RJ45/2RJ45-PM is not signed by an authority known to the client (as shipped, they are not), then interactive SSL clients such as web browsers will generally warn the user.
- If the name in server authentication certificate does not match the *hostname* that was used to access the server, then interactive SSL clients such as web browsers will generally warn the user.

6.3.6.2. Client Authentication

Client Authentication is the mechanism by which the ICDM-RX/TCP-16RJ45/2RJ45-PM verifies the identity of clients (that is, web browsers and so forth).

- Clients can generally be configured to accept a particular unknown server certificate so that the user is not subsequently warned.
- The ICDM-RX/TCP-16RJ45/2RJ45-PM (generally an SSL server) can be configured by uploading a trusted *authority* certificate that will be used to verify the ID certificates presented to the ICDM-RX/TCP-16RJ45/2RJ45-PM by SSL clients. This allows you to restrict access to the ICDM-RX/TCP-16RJ45/2RJ45-PM to a limited set of clients which have been configured with corresponding ID certificates.
- ICDM-RX/TCP-16RJ45/2RJ45-PM units will be shipped without an authority certificate and will not require clients to present ID certificates. This allows any and all SSL clients to connect to the ICDM-RX/TCP-16RJ45/2RJ45-PM.

6.3.6.3. Certificates and Keys

To control access to the ICDM-RX/TCP-16RJ45/2RJ45-PM's SSL/TLS protected resources you should create your own custom CA certificate and then configure authorized client applications with identity certificates signed by the custom CA certificate.

This uploaded CA certificate that is used to validate a client's identity is sometimes referred to as a *trusted root certificate*, a *trusted authority certificate*, or a *trusted CA certificate*. This CA certificate might be that of a trusted commercial certificate authority or it may be a privately generated certificate that an organization creates internally to provide a mechanism to control access to resources that are protected by the SSL/TLS protocols.

The following is a list that contains additional information about certificates and keys:

- By default, the ICDM-RX/TCP-16RJ45/2RJ45-PM is shipped without a CA (Certificate Authority) and therefore allowing connections from any SSL/TLS client. If desired, controlled access to SSL/TLS protected features can be configured by uploading a client authentication certificate to the ICDM-RX/TCP-16RJ45/2RJ45-PM.

- Certificates can be obtained from commercial certificate authorities (VeriSign, Thawte, Entrust, and so forth.).
- Certificates can be created by users for their own use by using **openssl** command line tools or other applications.
- Certificates and keys to be uploaded to the ICDM-RX/TCP-16RJ45/2RJ45-PM must be in the **.DER** binary file format, not in the **.PEM** ASCII file format. (The **openssl** tools can create files in either format and can convert files back and forth between the two formats.)
- Configuring Certificates and keys are configured by four uploaded files on the bottom *Key and Certificate Management* portion of the *Edit Security Configuration* web page:
  - **RSA Key Pair used by SSL and SSH servers**

    This is a private/public key pair that is used for two purposes:

    - It is used by some cipher suites to encrypt the SSL/TLS handshaking messages. Possession of the private portion of this key pair allows an eavesdropper to both decrypt traffic on SSL/TLS connections that use RSA encryption during handshaking.
    - It is used to sign the Server RSA Certificate in order to verify that the ICDM-RX/TCP-16RJ45/2RJ45-PM is authorized to use the server RSA identity certificate. Possession of the private portion of this key pair allows somebody to pose as the ICDM-RX/TCP-16RJ45/2RJ45-PM.

    If the Server RSA Key is replaced, a corresponding RSA server certificate must also be generated and uploaded as a matched set or clients are not able to verify the identity certificate.
  - **RSA Server Certificate used by SSL servers**

    - This is the RSA identity certificate that the ICDM-RX/TCP-16RJ45/2RJ45-PM uses during SSL/TLS handshaking to identify itself. It is used most frequently by SSL server code in the ICDM-RX/TCP-16RJ45/2RJ45-PM when clients open connections to the ICDM-RX/TCP-16RJ45/2RJ45-PM's secure web server or other secure TCP ports. If an ICDM-RX/TCP-16RJ45/2RJ45-PM serial port configuration is set up to open (as a client), a TCP connection to another server device, the ICDM-RX/TCP-16RJ45/2RJ45-PM also uses this certificate to identify itself as an SSL client if requested by the server.
    - In order to function properly, this certificate must be signed using the Server RSA Key. This means that the server RSA certificate and server RSA key must be replaced as a pair.
  - **DH Key pair used by SSL servers**

    This is a private/public key pair that is used by some cipher suites to encrypt the SSL/TLS handshaking messages.

    Possession of the private portion of the key pair allows an eavesdropper to decrypt traffic on SSL/TLS connections that use DH encryption during handshaking.
  - **Client Authentication Certificate used by SSL servers**

    If configured with a CA certificate, the ICDM-RX/TCP-16RJ45/2RJ45-PM requires all SSL/TLS clients to present an RSA identity certificate that has been signed by the configured CA certificate. As shipped, the ICDM-RX/TCP-16RJ45/2RJ45-PM is not configured with a CA certificate and all SSL/TLS clients are allowed.

6.3.7. SSL Performance

The ICDM-RX/TCP-16RJ45/2RJ45-PM has these SSL performance characteristics:

- Encryption/decryption is a CPU-intensive process, and using encrypted data streams will limit the number of ports that can be maintained at a given serial throughput. For example, the table below shows the number of ports that can be maintained by SocketServer at 100% throughput for various cipher suites and baud rates.

	9600	38400	57600	115200
RC4-MD5	32	16	10	5
RC4-SHA	32	13	9	4
AES128-SHA	28	7	5	2
AES256-SHA	26	7	4	2
DES3-SHA	15	3	2	1

Note: *These throughputs required 100% CPU usage, so other features such as the web server are very unresponsive at the throughputs shown above. To maintain a usable web interface, one would want to stay well below the maximum throughput/port numbers above.*

- The overhead required to set up an SSL connection is significant. The time required to open a connection to SocketServer varies depending on the public-key encryption scheme used for the initial handshaking. These are typical setup times for the three public-key encryption schemes for the ICDM-RX/TCP-16RJ45/2RJ45-PM:
  - RSA 0.66 seconds
  - DHE 3.84 seconds
  - DHA 3.28 seconds
- Since there is a certain amount of overhead for each block of data sent/received on an SSL connection, the SocketServer polling rate and size of bocks that are written to the SocketServer also has a noticeable effect on CPU usage. Writing larger blocks of data and a slower SocketServer polling rate will decrease CPU usage and allow somewhat higher throughputs.

6.3.8. SSL Cipher Suites

This subsection provides information about SSL cipher suites.

- An SSL connection uses four different facilities, each of which can use one of several different ciphers or algorithms. A particular combination of four ciphers/algorithms is called a “cipher suite”.
- A Cipher Suite consists of
  - Public Key Encryption Algorithm
    - Used to protect the initial handshaking and connection setup.
    - Typical options are RSA, DH, DHA, DHE, EDH, SRP, PSK. The ICDM-RX/TCP-16RJ45/2RJ45-PM supports RSA, DHA, DHE.
  - Authentication Algorithm
    - Used to verify the identities of the two parties to each other.
    - Typical options are RSA, DSA, ECDSA. The ICDM-RX/TCP-16RJ45/2RJ45-PM supports only RSA.
  - Stream Cipher
    - Used to encrypt the user-data exchanged between the two parties.
    - Typical options: RC4, DES, 3DES, AES, IDEA, Camellia, NULL. The ICDM-RX/TCP-16RJ45/2RJ45-PM supports RC4, 3DES, AES.

- Message Authentication Code
  - Hash function (checksum) used to verify that each message frame has not be corrupted or changed while in transit.
  - Typical options include MD5, SHA, MD2, MD4. The ICDM-RX/TCP-16RJ45/2RJ45-PM supports MD5, SHA

- In the design of the SSL/TLS protocols the choices of four of the above are not independent of each other: only certain combinations are defined by the standards. The standard combinations of protocol (SSL or TLS) and cipher suites support by ICDM-RX/TCP-16RJ45/2RJ45-PM are shown in the following table.

6.3.9. ICDM-RX/TCP-16RJ45/2RJ45-PM Supported Cipher Suites

The ICDM-RX/TCP-16RJ45/2RJ45-PM supports the cipher suites:

Protocol	Public Key	Authentication	Cipher	MAC
SSL	RSA	RSA	3DES	SHA
SSL	RSA	RSA	RC4	SHA
SSL	RSA	RSA	RC4	MD5
SSL	DHE	RSA	3DES	SHA
SSL	DHA	RSA	RC4	MD5
SSL	RSA	RSA	NULL	MD5
SSL	RSA	RSA	NULL	SHA
TLS	RSA	RSA	AES128	SHA
TLS	RSA	RSA	AES256	SHA
TLS	DHE	RSA	AES128	SHA
TLS	DHE	RSA	AES256	SHA
TLS	DHA	RSA	AES128	SHA
TLS	DHA	RSA	AES256	SHA

6.3.9.1. SSL Resources

You can refer to the following SSL resources for more information:

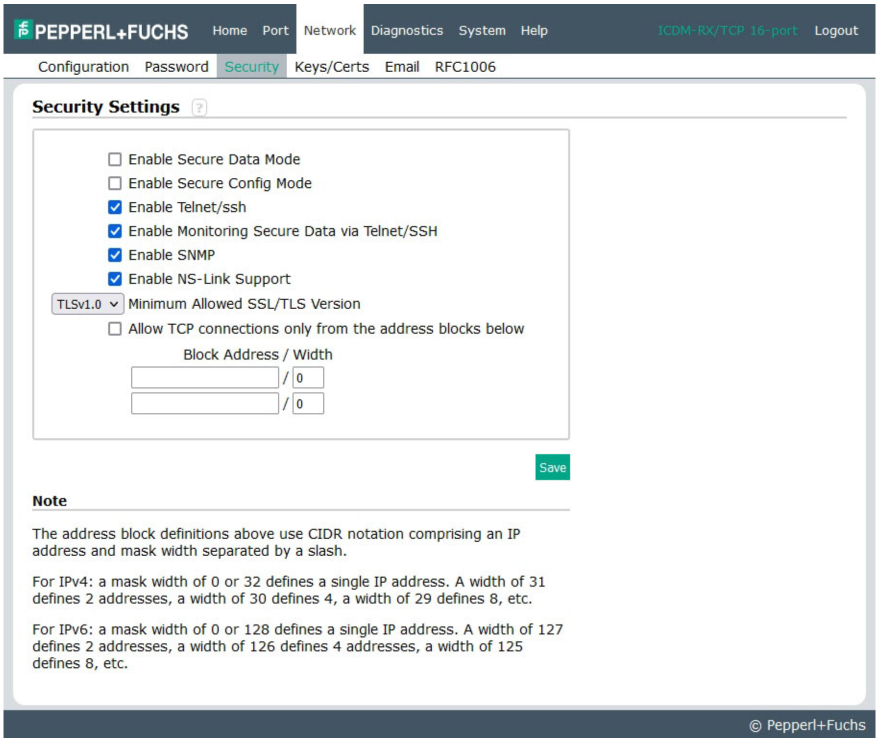
- Standard reference book is SSL and TLS by Eric Rescorla
- Wikipedia page on SSL/TLS provides a good overview: http://en.wikipedia.org/wiki/TLS
- **openssl** contains command-line tools to do the following. More information is available at: http://www.openssl.org/
  - Create/examine keys/certificates
  - Act as client or server
- **ssldump** is a -command line tool that displays a human-readable dump of an SSL connection's handshaking and traffic:. More information can be found at: http://www.rtfm.com/ssldump/.
  - If provided with server's private key, can decrypt data stream
  - Can display decoded data stream in ASCII/hex
  - Can display contents of handshaking packets (including ID certificates)

6.4. Configure/Enable Security Features Overview

You can enable ICDM-RX/TCP-16RJ45/2RJ45-PM security features the web page (SocketServer or the NS-Link version). *Key and Certificate Management* must be done using the *Security* tab in the ICDM-RX/TCP-16RJ45/2RJ45-PM web pages.

If you want secure COM ports, you must also **Enable SSL Mode** and enter any applicable server or client certificates in the NS-Link device driver for Windows. See *Device Driver (NS-Link) Installation* on Page 17.

The following illustration shows the **Security Settings** page under the **Network** menu and is discussed in the following table.



Security Settings

☐ Enable Secure Data Mode
☐ Enable Secure Config Mode
☑ Enable Telnet/ssh
☑ Enable Monitoring Secure Data via Telnet/SSH
☑ Enable SNMP
☑ Enable NS-Link Support
TLSv1.0 Minimum Allowed SSL/TLS Version
☐ Allow TCP connections only from the address blocks below

Block Address	Width
	0
	0

Note

The address block definitions above use CIDR notation comprising an IP address and mask width separated by a slash.

For IPv4: a mask width of 0 or 32 defines a single IP address. A width of 31 defines 2 addresses, a width of 30 defines 4, a width of 29 defines 8, etc.

For IPv6: a mask width of 0 or 128 defines a single IP address. A width of 127 defines 2 addresses, a width of 126 defines 4 addresses, a width of 125 defines 8, etc.

Security Option Descriptions	
Enable Secure Data Mode	If **Secure Data Mode** is enabled TCP connections which carry data to/from the serial ports will be encrypted using SSL or TLS security protocols. This includes the following: • TCP connections to the per-serial-port TCP ports (default is 8000, 8001, 8002, and so forth) are encrypted using SSL/TLS. • TCP connections to TCP Port 4606 on which the ICDM-RX/TCP-16RJ45/2RJ45-PM implements the Pepperl+Fuchs proprietary serial driver protocol are encrypted using SSL/TLS. • Since SSL/TLS can not be used for either UDP data streams or for the Pepperl+Fuchs proprietary MAC mode Ethernet driver protocol, both UDP and MAC mode serial data transport features are disabled. • In order to minimize possible security problems, e-mail and RFC1006 features are also disabled in *Secure Data* mode. In addition to encrypting the data streams, it is possible to configure the ICDM-RX/TCP-16RJ45/2RJ45-PM so that only authorized client applications can connect using SSL/TLS. See the *Client Authentication* discussion on Page 44 for details.
Enable Secure Config Mode	If **Secure Config Mode** is enabled, unencrypted access to administrative and diagnostic functions is disabled. **Secure Config Mode** changes ICDM-RX/TCP-16RJ45/2RJ45-PM behavior as follows: • Telnet access to administrative and diagnostic functions is disabled. SSH access is still allowed. • Unencrypted access to the web server via Port 80 (http://URLs) is disabled. • Encrypted access to the web server via Port 443 (https://URLs) is still allowed. • Administrative commands that change configuration or operating state which are received using the Pepperl+Fuchs proprietary TCP driver protocol on TCP Port 4606 are ignored. • Administrative commands that change configuration or operating state that are received using the Pepperl+Fuchs MAC mode proprietary Ethernet protocol number 0x11FE are ignored.

Security Option Descriptions (Continued)	
Enable Monitoring Secure Data via Telnet	When checked, this allows the monitor command to be used while **Secure Data Mode** is enabled. When unchecked, the monitor command can only be used if **Secure Data Mode** is not enabled. You must click **Save** and reboot the ICDM-RX/TCP-16RJ45/2RJ45-PM for the change to go into affect. This option is disabled by default. The **Enable Monitoring Secure Data via Telnet** feature allows you to monitor serial data being sent/received on a serial port (either via NS-Link or SocketServer). The monitoring is done by telnetting to the ICDM-RX/TCP-16RJ45/2RJ45-PM and using the following commands: • **monitor [-ac] portnumber** Display a live hex dump of TX/RX data for the specified serial port. You can only monitor one port at a time. The live dump will continue until the **Enter** key is pressed. See the following detailed description and examples. The data is logged when it is written/read to/from the serial port driver's TX/RX buffers -- as such, the relative timing between RX/TX bytes is not precise, but it should be sufficient to debug most problems (especially frame-oriented, command/response serial protocols). Monitoring serial data through a telnet connection does generate extra network traffic and may have small effects on the timing of ICDM-RX/TCP-16RJ45/2RJ45-PM operations when large amounts of data are being logged at high baud rates. See *Example 1* on Page 51 for more information. - The **-a** option enables displaying of ASCII representation of data in a column to the right the hex representation. See *Example 2* on Page 51. - The **-c** option enables the use of color instead of < and > to indicate the data flow direction. Tx is green and Rx is red. See *Example 3* on Page 52. • **securemon [enable|disable]** By default, monitoring of TX/RX data when in **Secure Data Mode** is not allowed through telnet (an insecure protocol). This command allows you to override that default when **securemon** is enabled it will allow monitoring of secure data via an insecure protocol like telnet. ***Note:*** *Optionally, you can use the Port Monitor function in the web interface. Click* **Diagnostics | Port Monitor**.
Enable Telnet/ssh	This option enables or disables the telnet security feature after you click **Save** and the ICDM-RX/TCP-16RJ45/2RJ45-PM has been rebooted. *This option is enabled by default.*
Enable SNMP	This option enables or disables the SNMP security feature after you click **Save** and the ICDM-RX/TCP-16RJ45/2RJ45-PM has been rebooted. *This option is enabled by default*.
Minimum Allowed SSL/TLS Version	You can select the appropriate version for your environment. • SSLv3.0 • TLSv1.0 (default) • TLSv1.1 • TLSv1.2
Allow TCP connections only from the address blocks below	When you select this option, you must enter the Block Address and width of the TCP connections that you want to communicate with this ICDM-RX/TCP-16RJ45/2RJ45-PM.

6.4.1. Example 1

The following example shows how to monitor output using a loopback plug and a program that repeatedly sends the string abcABC123 to Port 1:

```
dm> monitor 1
Serial monitoring started for port 1 -- press [Enter] to stop.
> 61 62 63 41 42 43 31 32 33
< 61 62 63 41 42 43 31 32 33
> 61 62 63 41 42 43 31 32 33
< 61 62 63 41 42 43 31 32 33
> 61 62 63 41 42 43 31 32 33
< 61 62 63 41 42 43 31 32 33
> 61 62 63 41 42 43 31 32 33
< 61 62 63 41 42 43 31 32 33
```

6.4.2. Example 2

The following example shows how the **-a** option enables displaying of ASCII representation of data in a column to the right the hex representation:

```
dm> monitor -a 1
Serial monitoring started for port 1 -- press [Enter] to stop.
> 61 62 63 41 42 43 31 32 33             > abcABC123
< 61 62 63 41 42 43 31 32 33             < abcABC123
> 61 62 63 41 42 43 31 32 33             > abcABC123
< 61 62 63 41 42 43 31 32 33             < abcABC123
> 61 62 63 41 42 43 31 32 33             > abcABC123
< 61 62 63 41 42 43 31 32 33             < abcABC123
> 61 62 63 41 42 43 31 32 33             > abcABC123
< 61 62 63 41 42 43 31 32 33             < abcABC123
> 61 62 63 41 42 43 31 32 33             > abcABC123
< 61 62 63 41 42 43 31 32 33             < abcABC123
> 61 62 63 41 42 43 31 32 33             > abcABC123
< 61 62 63 41 42 43 31 32 33             < abcABC123
```

6.4.3. Example 3

The **-c** option enables the use of color instead of < and > to indicate the data flow direction. Tx is green and Rx is red.

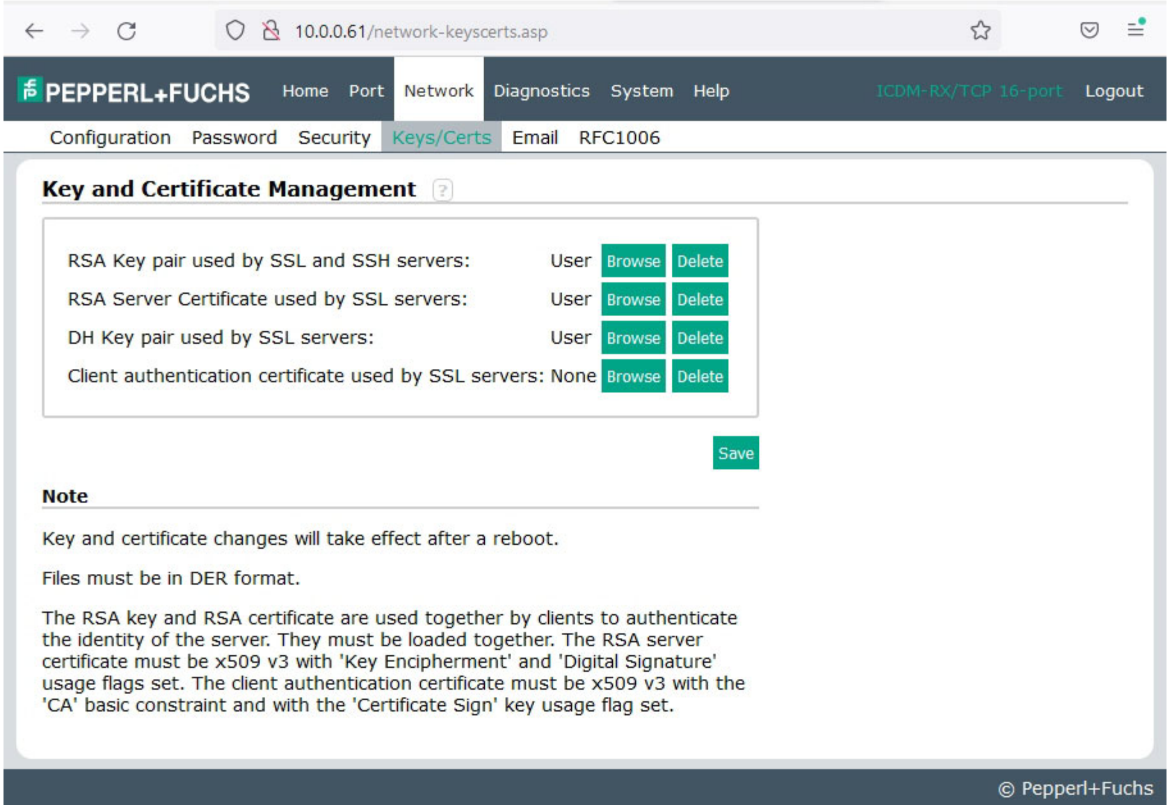
```
dm> monitor -c 1
Serial monitoring started for port 1 -- press [Enter] to stop.
61 62 63 41 42 43 31 32 33 61 62 63 41 42 43 31
32 33 61 62 63 41 42 43 31 32 33 61 62 63 41 42
43 31 32 33 61 62 63 41 42 43 31 32 33 61 62 63
41 42 43 31 32 33 61 62 63 41 42 43 31 32 33 61
62 63 41 42 43 31 32 33 61 62 63 41 42 43 31 32
33 61 62 63 41 42 43 31 32 33 61 62 63 41 42 43
31 32 33 61 62 63 41 42 43 31 32 33 61 62 63 41
42 43 31 32 33 61 62 63 41 42 43 31 32 33 61 62
63 41 42 43 31 32 33 61 62 63 41 42 43 31 32 33
```

The -a and -c options can be used together:

```
dm> monitor -ac 1
Serial monitoring started for port 1 -- press [Enter] to stop.
61 62 63 41 42 43 31 32 33 61 62 63 41 42 43 31  | abcABC123abcABC1
32 33 61 62 63 41 42 43 31 32 33 61 62 63 41 42  | 23abcABC123abcAB
43 31 32 33 61 62 63 41 42 43 31 32 33 61 62 63  | C123abcABC123abc
41 42 43 31 32 33 61 62 63 41 42 43 31 32 33 61  | ABC123abcABC123a
62 63 41 42 43 31 32 33 61 62 63 41 42 43 31 32  | bcABC123abcABC12
33 61 62 63 41 42 43 31 32 33 61 62 63 41 42 43  | 3abcABC123abcABC
31 32 33 61 62 63 41 42 43 31 32 33 61 62 63 41  | 123abcABC123abcA
42 43 31 32 33 61 62 63 41 42 43 31 32 33 61 62  | BC123abcABC123ab
63 41 42 43 31 32 33 61 62 63 41 42 43 31 32 33  | cABC123abcABC123
```

6.4.4. Key and Certificate Management

Key and Certificate management is only available in the **Network | Keys/Cert** web page.



Key and Certificate Management

RSA Key pair used by SSL and SSH servers:	User	Browse	Delete
RSA Server Certificate used by SSL servers:	User	Browse	Delete
DH Key pair used by SSL servers:	User	Browse	Delete
Client authentication certificate used by SSL servers:	None	Browse	Delete

Save

Note

Key and certificate changes will take effect after a reboot.

Files must be in DER format.

The RSA key and RSA certificate are used together by clients to authenticate the identity of the server. They must be loaded together. The RSA server certificate must be x509 v3 with 'Key Encipherment' and 'Digital Signature' usage flags set. The client authentication certificate must be x509 v3 with the 'CA' basic constraint and with the 'Certificate Sign' key usage flag set.

© Pepperl+Fuchs

Key and Certificate Management Option Descriptions	
RSA Key pair used by SSL and SSH servers	This is a private/public key pair that is used for two purposes: It is used by some cipher suites to encrypt the SSL/TLS handshaking messages. Possession of the private portion of this key pair allows an eavesdropper to both decrypt traffic on SSL/TLS connections that use RSA encryption during handshaking. It is used to sign the Server RSA Certificate in order to verify that the ICDM-RX/TCP-16RJ45/2RJ45-PM is authorized to use the server RSA identity certificate. Possession of the private portion of this key pair allows somebody to pose as the ICDM-RX/TCP-16RJ45/2RJ45-PM. If the Server RSA Key is to be replaced, a corresponding RSA identity certificate must also be generated and uploaded or clients are not able to verify the identity certificate.

Key and Certificate Management Option Descriptions (Continued)	
RSA Server Certificate used by SSL servers	This is the RSA identity certificate that the ICDM-RX/TCP-16RJ45/2RJ45-PM uses during SSL/TLS handshaking to identify itself. It is used most frequently by SSL server code in the ICDM-RX/TCP-16RJ45/2RJ45-PM when clients open connections to the ICDM-RX/TCP-16RJ45/2RJ45-PM's secure web server or other secure TCP ports. If an ICDM-RX/TCP-16RJ45/2RJ45-PM serial port configuration is set up to open (as a client) a TCP connection to another server device, the ICDM-RX/TCP-16RJ45/2RJ45-PM also uses this certificate to identify itself as an SSL client if requested by the server. In order to function properly, this certificate must be signed using the Server RSA Key. This means that the server RSA certificate and server RSA key must be replaced as a pair.
DH Key pair used by SSL servers	This is a private/public key pair that is used by some cipher suites to encrypt the SSL/TLS handshaking messages. ***Note:*** *Possession of the private portion of the key pair allows an eavesdropper to decrypt traffic on SSL/TLS connections that use DH encryption during handshaking.*
Client Authentication Certificate used by SSL servers	If configured with a CA certificate, the ICDM-RX/TCP-16RJ45/2RJ45-PM requires all SSL/TLS clients to present an RSA identity certificate that has been signed by the configured CA certificate. As shipped, the ICDM-RX/TCP-16RJ45/2RJ45-PM is not configured with a CA certificate and all SSL/TLS clients are allowed. See *Client Authentication* on Page 44 for more detailed information
• *All ICDM-RX/TCP-16RJ45/2RJ45-PM units are shipped from the factory with identical configurations. They all have the identical, self-signed, Pepperl+Fuchs Server RSA Certificates, Server RSA Keys, Server DH Keys, and no Client Authentication Certificates*. • *For maximum data and access security, you should configure all ICDM-RX/TCP-16RJ45/2RJ45-PM units with custom certificates and keys*.	

6.5. Using a Web Browser to Set Security Features

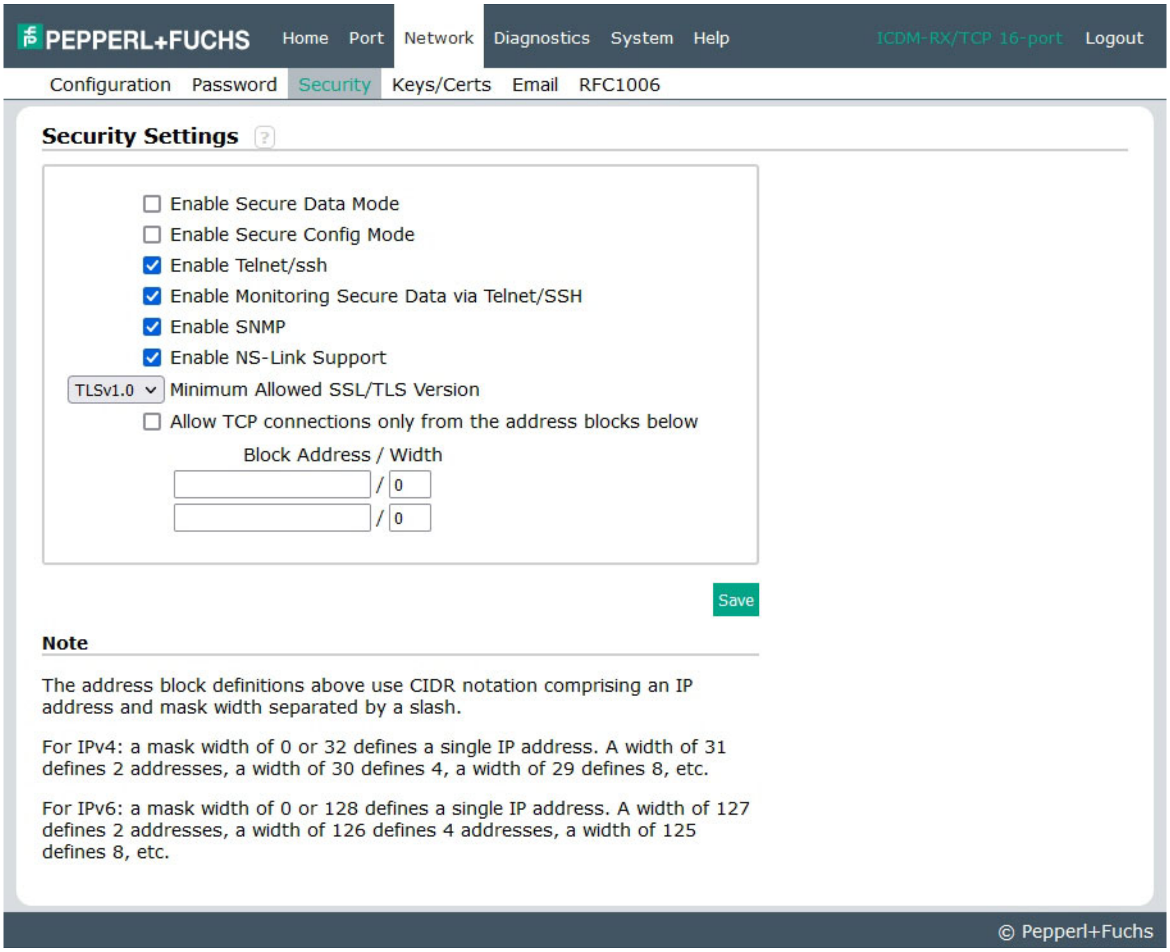
The follow procedures are discussed below:

- *Changing Security Configuration*
- *Changing Keys and Certificates* on Page 56

6.5.1. Changing Security Configuration

Use the following steps to change security settings in the ICDM-RX/TCP-16RJ45/2RJ45-PM.

1. Enter the IP address of the ICDM-RX/TCP-16RJ45/2RJ45-PM in the *Address* field of your web browser and press the **Enter** key.
2. Click **Network | Security**.
3. Click the appropriate check boxes to enable or disable security for your environment.


PEPPERL+FUCHS
Home Port Network Diagnostics System Help
ICDM-RX/TCP 16-port
Logout
Configuration Password Security Keys/Certs Email RFC1006

Security Settings

□ Enable Secure Data Mode
□ Enable Secure Config Mode
☑ Enable Telnet/ssh
☑ Enable Monitoring Secure Data via Telnet/SSH
☑ Enable SNMP
☑ Enable NS-Link Support
TLSv1.0 Minimum Allowed SSL/TLS Version
□ Allow TCP connections only from the address blocks below

Block Address / Width
/ 0
/ 0

Save

Note

The address block definitions above use CIDR notation comprising an IP address and mask width separated by a slash.

For IPv4: a mask width of 0 or 32 defines a single IP address. A width of 31 defines 2 addresses, a width of 30 defines 4, a width of 29 defines 8, etc.

For IPv6: a mask width of 0 or 128 defines a single IP address. A width of 127 defines 2 addresses, a width of 126 defines 4 addresses, a width of 125 defines 8, etc.

Refer to the help system or *Configure/Enable Security Features Overview* on Page 48 for detailed information.

4. After making changes, click **Save.**

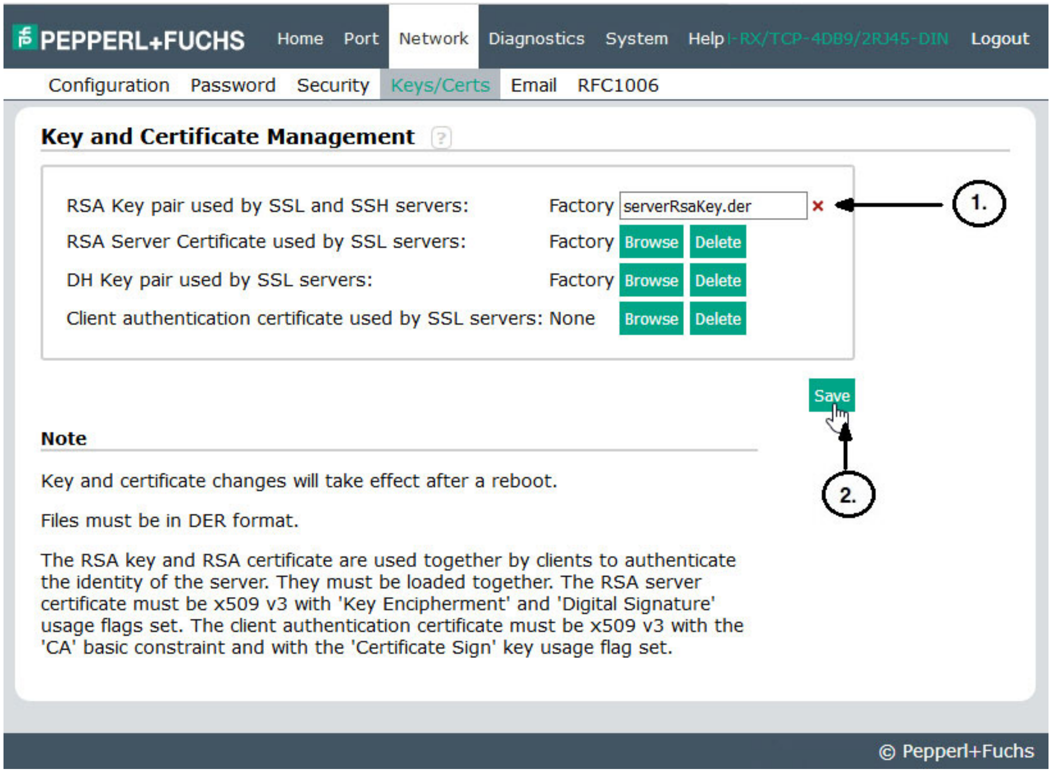
6.5.2. Changing Keys and Certificates

Use the following steps to update security keys and certificates in the ICDM-RX/TCP-16RJ45/2RJ45-PM. Refer to the help system or *Key and Certificate Management* subsection on Page 56 for detailed information.

1. If necessary, enter the IP address of the ICDM-RX/TCP-16RJ45/2RJ45-PM in the *Address* field of your web browser and press the **Enter** key.
2. Click **Network | Keys/Certs**.
3. Click **Browse** to locate the key or certificate file, highlight the file, and click **Open**.
4. Click **Upload**.
5. Click **Save**, but changes will not take effect until the ICDM-RX/TCP-16RJ45/2RJ45-PM is rebooted.

   Note: *The key or certificate notation changes from factory or none to* ***User*** *when the ICDM-RX/TCP-16RJ45/2RJ45-PM is secure.*

   You can reboot the ICDM-RX/TCP-16RJ45/2RJ45-PM by clicking **System | Reboot** or use the PortVision DX reboot option.



Key and Certificate Management

RSA Key pair used by SSL and SSH servers:	Factory	serverRsaKey.der ✕
RSA Server Certificate used by SSL servers:	Factory	Browse Delete
DH Key pair used by SSL servers:	Factory	Browse Delete
Client authentication certificate used by SSL servers:	None	Browse Delete

Note

Key and certificate changes will take effect after a reboot.

Files must be in DER format.

The RSA key and RSA certificate are used together by clients to authenticate the identity of the server. They must be loaded together. The RSA server certificate must be x509 v3 with 'Key Encipherment' and 'Digital Signature' usage flags set. The client authentication certificate must be x509 v3 with the 'CA' basic constraint and with the 'Certificate Sign' key usage flag set.

6.6. Password Authentication

This section discusses three methods of configuring password authentication.

- Using the web page
- Using telnet or SSH

6.6.1. Using the Web Page

You can easily set up a password to secure the ICDM-RX/TCP-16RJ45/2RJ45-PM. Use the following procedure to configure a password using the web page.

Note: *There is no password set from the factory.*

Use the following information to configure a password for this ICDM-RX/TCP-16RJ45/2RJ45-PM.

1. Log into the ICDM-RX/TCP-16RJ45/2RJ45-PM using your web browser and the IP address of the ICDM-RX/TCP-16RJ45/2RJ45-PM.
2. Click **Network | Password**.
3. If changing an existing password, enter that password in the **Old Password** field.
4. Enter a new password and enter the confirmation password.
5. Click the **Save** button.

When anyone attempts to log into the ICDM-RX/TCP-16RJ45/2RJ45-PM, you must enter the following:

- admin for the username
- The configured password for the password

6.6.2. Using Telnet or SSH

If you have not done so, install PortVision DX, which is a Windows application. If necessary, you can download from https://www.pepperl-fuchs.com the latest version of PortVision DX and install that version.

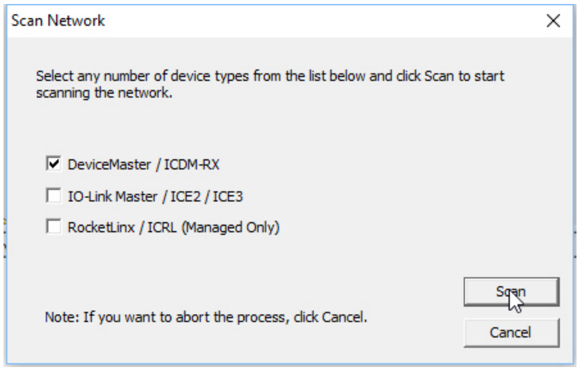
This subsection discusses the following topics:

- *Login Authentication* on Page 57
- *Configuring Passwords* on Page 59
- *Telnet Commands* on Page 61

6.6.2.1. Login Authentication

Use the following steps to access a telnet session in PortVision DX so that you can set the log-in authentication.

1. Start PortVision DX.
2. If this is the first time you have started PortVision DX:
   a. Click the **Scan** button on the Toolbar to locate the ICDM-RX/TCP-16RJ45/2RJ45-PM for which you want to configure password authentication.
   b. Click the ICDM-RX/TCP-16RJ45/2RJ45-PM option or other appropriate models.
   c. Click the **Scan** button.

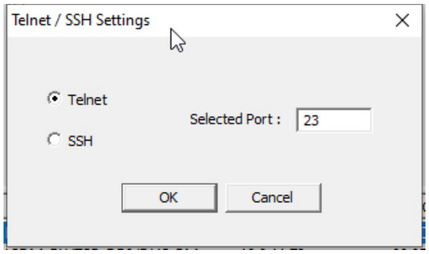


Select any number of device types from the list below and click Scan to start scanning the network.

☑ DeviceMaster / ICDM-RX
☐ IO-Link Master / ICE2 / ICE3
☐ RocketLinx / ICRL (Managed Only)

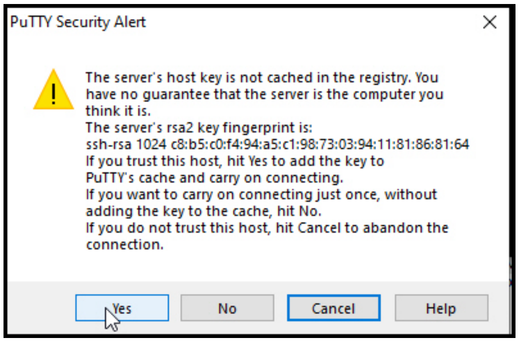
Note: If you want to abort the process, click Cancel.

3. RIght-click the ICDM-RX/TCP-16RJ45/2RJ45-PM that you want to configure for password authentication and click **Telnet / SSH Session**.
4. Click the **Telnet** or **SSH** option, leave the **Selected Port** number as 23 or 22, and click **Ok**.



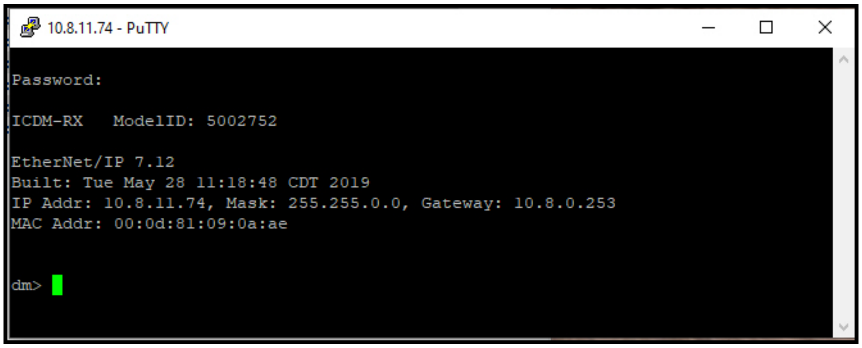
● Telnet
○ SSH
Selected Port : 23

5. If you select **SSH**, click **Yes** to the *PuTTY Security Alert.*



The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 c8:b5:c0:f4:94:a5:c1:98:73:03:94:11:81:86:81:64
If you trust this host, hit Yes to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the
connection.

6. If this is a Telnet session and the ICDM-RX/TCP-16RJ45/2RJ45-PM has a password configured, type the password and press Enter.

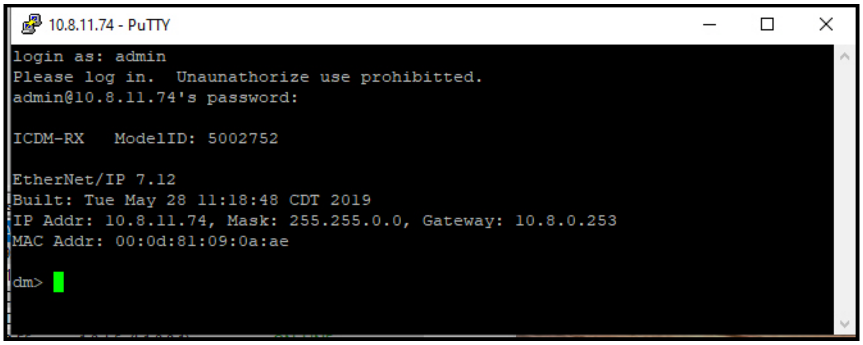


```
Password:

ICDM-RX   ModelID: 5002752

EtherNet/IP 7.12
Built: Tue May 28 11:18:48 CDT 2019
IP Addr: 10.8.11.74, Mask: 255.255.0.0, Gateway: 10.8.0.253
MAC Addr: 00:0d:81:09:0a:ae


dm>
```

Note: *If a password has not been configured, press Enter.*

4/27/22

If this is an SSH session, type admin for the login and the ICDM-RX/TCP-16RJ45/2RJ45-PM has a password configured, type the password and press Enter

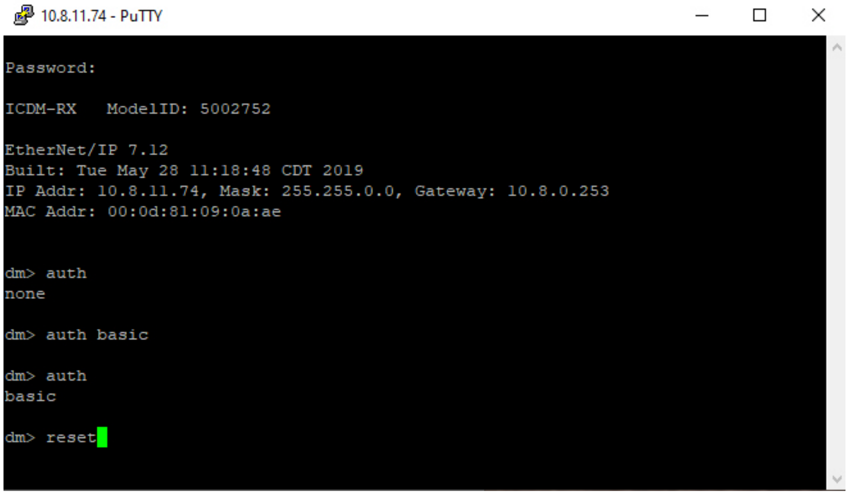


```
login as: admin
Please log in.  Unaunathorize use prohibited.
admin@10.8.11.74's password:

ICDM-RX   ModelID: 5002752

EtherNet/IP 7.12
Built: Tue May 28 11:18:48 CDT 2019
IP Addr: 10.8.11.74, Mask: 255.255.0.0, Gateway: 10.8.0.253
MAC Addr: 00:0d:81:09:0a:ae

dm>
```

7. Type **auth** and press Enter to see the authentication status, none indicates that there is no authentication set.
8. Type **auth** basic and press Enter to enable enforcing log-in functionality.
9. Type **reset** and press Enter.
10. Close the PuTTY window.

    PortVision DX temporarily displays that ICDM-RX/TCP-16RJ45/2RJ45-PM as OFF-LINE until the next polling cycle because the ICDM-RX/TCP-16RJ45/2RJ45-PM is rebooting.

To disable enforcing log-in functionality, type **auth none**.

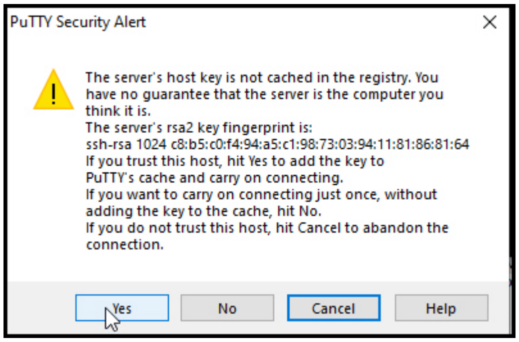


```
Password:

ICDM-RX   ModelID: 5002752

EtherNet/IP 7.12
Built: Tue May 28 11:18:48 CDT 2019
IP Addr: 10.8.11.74, Mask: 255.255.0.0, Gateway: 10.8.0.253
MAC Addr: 00:0d:81:09:0a:ae


dm> auth
none

dm> auth basic

dm> auth
basic

dm> reset
```

6.6.2.2. Configuring Passwords

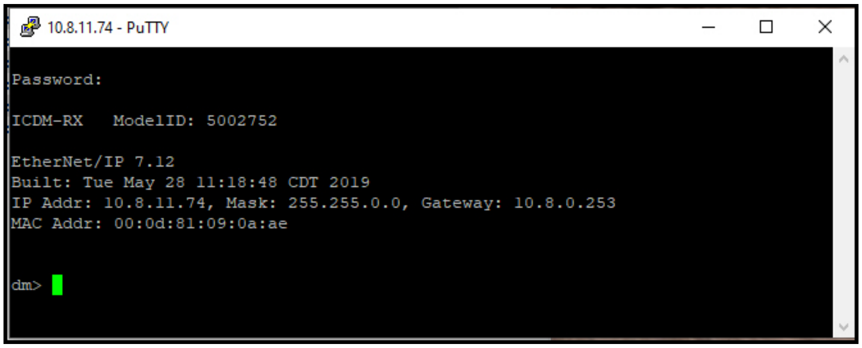
Use the following procedure to configure a ICDM-RX/TCP-16RJ45/2RJ45-PM password.

1. Highlight the ICDM-RX/TCP-16RJ45/2RJ45-PM that you want to configure for a password and click **Telnet / SSH Session**.
2. Click the Telnet or SSH option, leave the Selected Port number as 23, and click Ok.
3. If you select **SSH**, click **Yes** to the *PuTTY Security Alert.*



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 c8:b5:c0:f4:94:a5:c1:98:73:03:94:11:81:86:81:64
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

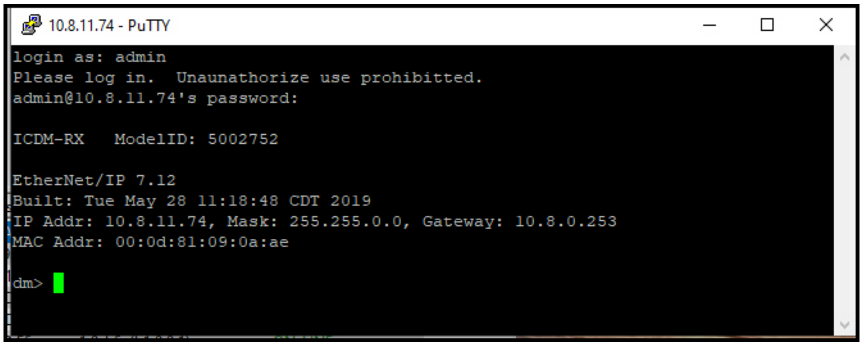
4. If this is a Telnet session and the ICDM-RX/TCP-16RJ45/2RJ45-PM has a password configured, type the password and press Enter.



```
Password:

ICDM-RX   ModelID: 5002752

EtherNet/IP 7.12
Built: Tue May 28 11:18:48 CDT 2019
IP Addr: 10.8.11.74, Mask: 255.255.0.0, Gateway: 10.8.0.253
MAC Addr: 00:0d:81:09:0a:ae


dm>
```

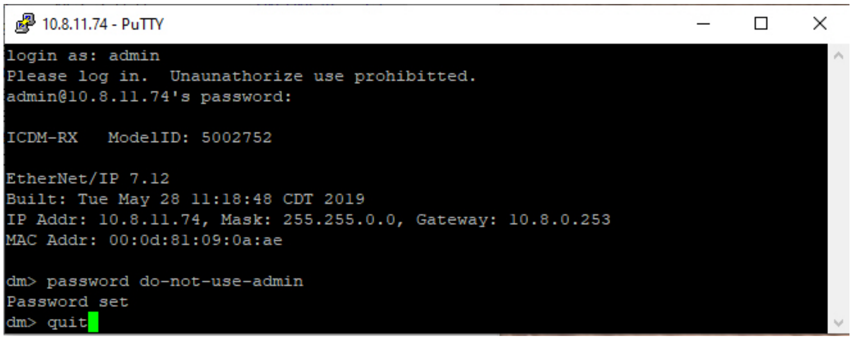
Note: *If a password has not been configured, press Enter.*

If this is an SSH session, type admin for the login and the ICDM-RX/TCP-16RJ45/2RJ45-PM has a password configured, type the password and press Enter



```
login as: admin
Please log in.  Unaunathorize use prohibitted.
admin@10.8.11.74's password:

ICDM-RX   ModelID: 5002752

EtherNet/IP 7.12
Built: Tue May 28 11:18:48 CDT 2019
IP Addr: 10.8.11.74, Mask: 255.255.0.0, Gateway: 10.8.0.253
MAC Addr: 00:0d:81:09:0a:ae

dm>
```

5. Type password and the password that you want to set. The example below shows setting the password to do-not-use-admin.



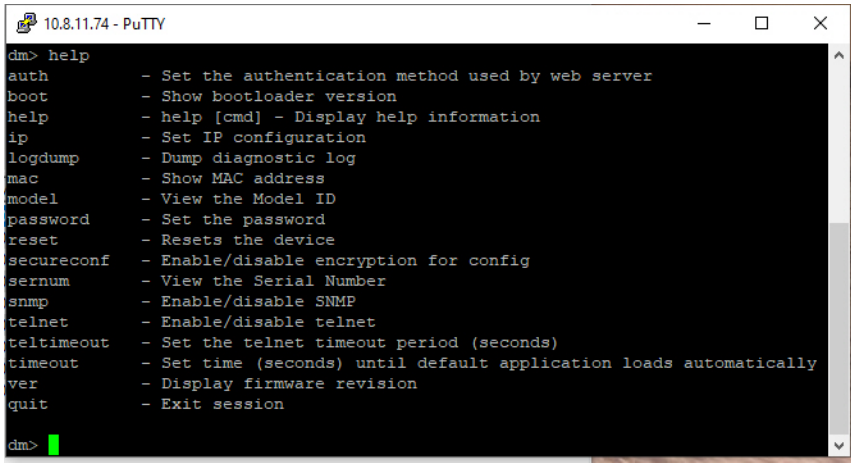
```
login as: admin
Please log in.  Unaunathorize use prohibitted.
admin@10.8.11.74's password:

ICDM-RX   ModelID: 5002752

EtherNet/IP 7.12
Built: Tue May 28 11:18:48 CDT 2019
IP Addr: 10.8.11.74, Mask: 255.255.0.0, Gateway: 10.8.0.253
MAC Addr: 00:0d:81:09:0a:ae

dm> password do-not-use-admin
Password set
dm> quit
```

Note: *Make sure that you do not forget the password because after you configure the ICDM-RX/TCP-16RJ45/2RJ45-PM with Secure Config Mode, you will not be able to recover the password and will need to return it to the factory to have the default setting loaded.*

6. Type **quit** and press Enter.

6.6.2.3. Telnet Commands

To access telnet help, type help.



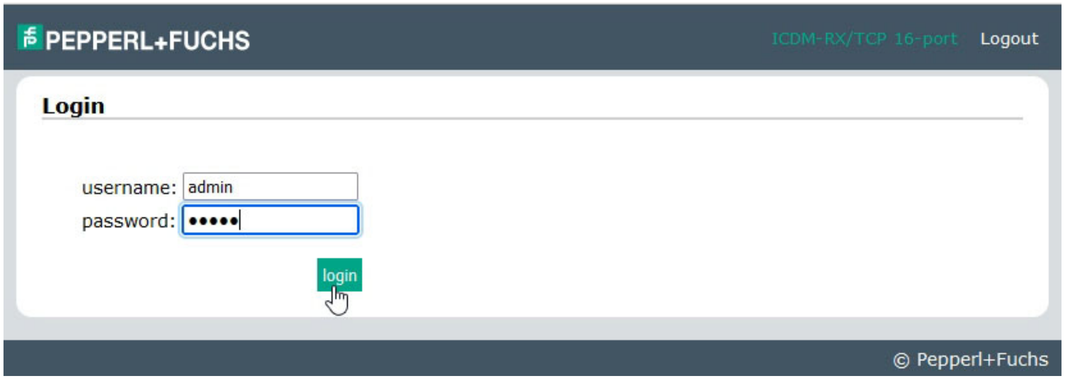
```
dm> help
auth          - Set the authentication method used by web server
boot          - Show bootloader version
help          - help [cmd] - Display help information
ip            - Set IP configuration
logdump       - Dump diagnostic log
mac           - Show MAC address
model         - View the Model ID
password      - Set the password
reset         - Resets the device
secureconf    - Enable/disable encryption for config
sernum        - View the Serial Number
snmp          - Enable/disable SNMP
telnet        - Enable/disable telnet
teltimeout    - Set the telnet timeout period (seconds)
timeout       - Set time (seconds) until default application loads automatically
ver           - Display firmware revision
quit          - Exit session

dm>
```

6.6.3. Web Page Password Access

When the authentication is set to require a password, such as basic, you will need to log into each web server session whether you use PortVision DX or a web browser.

Use these steps to log in:

1. Leave the User name blank.
2. Type in your password. If there is no password configured, leave the Password blank.
3. Click **OK**.



username: admin
password: •••••

Once logged in, you will have full read/write access to the wPROFINET IOeb pages.

7. Connecting Serial Devices

This section discusses connecting your serial devices to the ICDM-RX/TCP-16RJ45/2RJ45-PM. It also provides you with information to build serial cables and loopback connectors to test the serial ports.

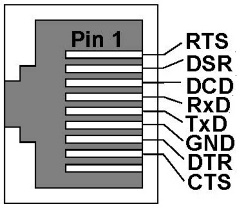
Use the appropriate subsection to connect asynchronous serial devices to the ICDM-RX/TCP-16RJ45/2RJ45-PM ports.

This subsection provides the following information:

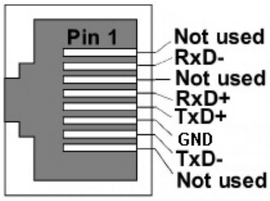
- Connector pin assignments (below)
- *RJ45 Null-Modem Cables (RS-232)* on Page 63
- *RJ45 Null-Modem Cables [RS-422/RS-485 (4-Wire)]* on Page 63
- *RJ45 Straight-Through Cables (RS-232/485)* on Page 63
- *RJ45 Loopback Plugs* on Page 64
- *RJ45 RS-485 Test Cable* on Page 64
- *Connecting RJ45 Devices* on Page 64

7.1. Connector Pin Out Assignments

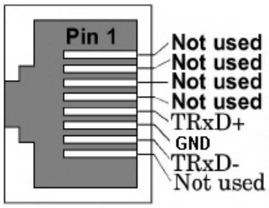
You can build your own null-modem or straight-through RJ45 serial cables if you are using the DB9 to RJ45 adapters using the following subsections.



RS-232



RS-422/RS-485 (4-Wire)

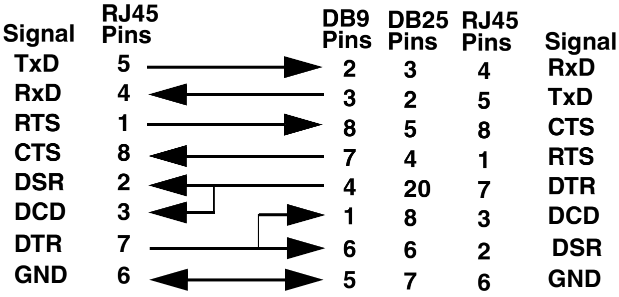


RS-485 (2-Wire)

Pin	RS-232	RS-422 RS-485 (4-Wire)	RS-485 (2-Wire)
1	RTS	Not used	Not used
2	DSR	RxD-	Not used
3	DCD	Not used	Not used
4	RxD	RxD+	Not used
5	TxD	TxD+	TxD/RxD+
6	GND	GND	GND
7	DTR	TxD-	TxD/RxD-
8	CTS	Not used	Not used

7.2. RJ45 Null-Modem Cables (RS-232)

Use the following figure if you need to build an RS-232 null-modem cable. A null-modem cable is required for connecting DTE devices.

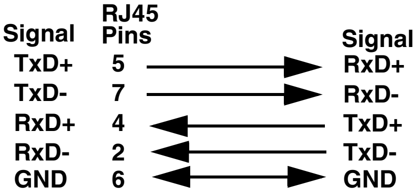


Signal	RJ45 Pins		DB9 Pins	DB25 Pins	RJ45 Pins	Signal
TxD	5	→	2	3	4	RxD
RxD	4	←	3	2	5	TxD
RTS	1	→	8	5	8	CTS
CTS	8	←	7	4	1	RTS
DSR	2	←	4	20	7	DTR
DCD	3	←	1	8	3	DCD
DTR	7	→	6	6	2	DSR
GND	6	↔	5	7	6	GND

Note: *You may want to purchase or build a straight-through cable and purchase a null-modem adapter. For example, a null-modem cable can be used to connect COM2 of one PC to COM2 of another PC.*

7.3. RJ45 Null-Modem Cables [RS-422/RS-485 (4-Wire)]

Use the following figure if you need to build an RS-422 or RS-485 (4-wire) null-modem RJ45 cable. A null-modem cable is required for connecting DTE devices.

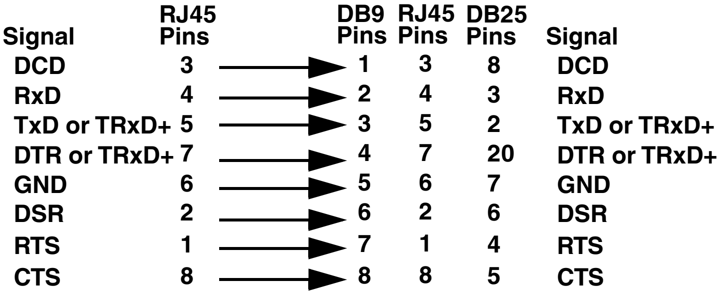


Signal	RJ45 Pins		Signal
TxD+	5	→	RxD+
TxD-	7	→	RxD-
RxD+	4	←	TxD+
RxD-	2	←	TxD-
GND	6	↔	GND

Note: *RS-422 pinouts are not standardized. Each peripheral manufacturer uses different pinouts. Please refer to the documentation for the peripheral to determine the pinouts for the signals above.*

7.4. RJ45 Straight-Through Cables (RS-232/485)

Use the following figure if you need to build an RS-232 or RS-485 straight-through cable. Straight-through cables are used to connect modems and other DCE devices. For example, a straight-through cable can be used to connect COM2 of one PC to COM2 to a modem.

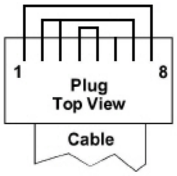


Signal	RJ45 Pins		DB9 Pins	RJ45 Pins	DB25 Pins	Signal
DCD	3	→	1	3	8	DCD
RxD	4	→	2	4	3	RxD
TxD or TRxD+	5	→	3	5	2	TxD or TRxD+
DTR or TRxD+	7	→	4	7	20	DTR or TRxD+
GND	6	→	5	6	7	GND
DSR	2	→	6	2	6	DSR
RTS	1	→	7	1	4	RTS
CTS	8	→	8	8	5	CTS

7.5. RJ45 Loopback Plugs

Loopback connectors are RJ45 serial port plugs with pins wired together that are used in conjunction with application software (Test Terminal for Windows, which is available in PortVision DX or Minicom for Linux) to test serial ports. The ICDM-RX/TCP-16RJ45/2RJ45-PM is shipped with a single loopback plug (RS-232/422).

- Pins 4 to 5
- Pins 1 to 8
- Pins 2 to 3 to 7

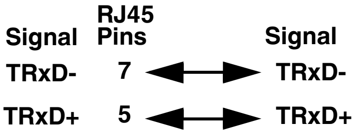


The RS-232 loopback plug also works for RS-422.

7.6. RJ45 RS-485 Test Cable

You can use a straight-through cable as illustrated previously, or build your own cable.

Note: *RS-422 pinouts are not standardized. Each peripheral manufacturer uses different pinouts. Refer to the documentation for the peripheral to determine the pinouts for the signals above.*



7.7. Connecting RJ45 Devices

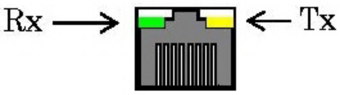
You can use this information to connect serial devices to RJ45 connectors.

1. Connect your serial devices to the appropriate serial port on the ICDM-RX/TCP-16RJ45/2RJ45-PM using the appropriate cable.

   Note: *Refer to the hardware manufacturer’s installation documentation if you need help with connector pinouts or cabling for the peripheral device.*

2. Verify that the ICDM-RX/TCP-16RJ45/2RJ45-PM LEDs indicate that the devices are communicating properly.

   The LED functions are displayed in the following table when the cable is attached properly to a serial device.



LED	Mode	Description	LED Status
RX (Green)	RS-232	No valid RS-232 device is connected	Always off
		Valid RS-232 device is connected but no data transmission is occurring	On
		Data being received	LED blinks
	RS-422/485	No data being received	Always off
		Data being received	LED blinks
	No mode	No mode selected	Always off
TX (Yellow)	RS-232/ 422/485	No data being transmitted	Always off
		Data being transmitted	LED blinks

3. You can refer to *ICDM-RX/TCP-16RJ45/2RJ45-PM LEDs* on Page 120 for information about the remaining LEDs.

Note: *The RX/TX LEDs cycle during a reboot cycle.*

8. Managing the ICDM-RX/TCP-16RJ45/2RJ45-PM

This section discusses the following ICDM-RX/TCP-16RJ45/2RJ45-PM maintenance procedures:

- *Rebooting the ICDM-RX/TCP-16RJ45/2RJ45-PM*
- *Uploading SocketServer to Multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs* on Page 67
- *Configuring Multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs Network Addresses* on Page 67

  Note: *You can configure the network addresses for multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs, configure common settings for the ICDM-RX/TCP-16RJ45/2RJ45-PMs, and save the settings to a configuration file that you can use to load settings up to all or selected ICDM-RX/TCP-16RJ45/2RJ45-PMs.*
- *Adding a New Device in PortVision DX* on Page 67
- *Using SocketServer Configuration Files* on Page 69
- *Using Driver Configuration Files* on Page 72
- *Changing the Bootloader Timeout* on Page 75, which discusses changing the Bootloader timeout
- *Managing Bootloader* on Page 77, which also discusses checking the Bootloader version and downloading the latest Bootloader
- *Checking the NS-Link Version* on Page 79
- *Restoring Serial Port Settings* on Page 79
- *Restoring Defaults* on Page 84
- *Accessing SocketServer Commands in Telnet/SSH Sessions (PortVision DX)* on Page 80
- *Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)* on Page 86

Note: *You can optionally refer to RedBoot Procedures on Page 88 if you want to perform procedures at the RedBoot level.*

8.1. Rebooting the ICDM-RX/TCP-16RJ45/2RJ45-PM

There are many ways to reboot the ICDM-RX/TCP-16RJ45/2RJ45-PM.

Method	Procedure
PortVision DX	Right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM or shift-click the ICDM-RX/TCP-16RJ45/2RJ45-PMs and click **Advanced >Reboot** and then **Yes**. ***Note:*** *If security has been enabled in the web page, you will need to reboot the ICDM-RX/TCP-16RJ45/2RJ45-PM in the web page.*
Web page	**System | Reboot:** You have 10 seconds to *Cancel* before the ICDM-RX/TCP-16RJ45/2RJ45-PM automatically reboots. Optionally, you can click **Reboot Now**.
Telnet	Type **reset**.
ICDM-RX/TCP-16RJ45/2RJ45-PM DIN Rail Models	ICDM-RX/TCP-16RJ45/2RJ45-PM DIN rail models have a **Reset/Restore** switch. • If the **Reset/Restore** switch is depressed for less than 2 seconds, the ICDM-RX/TCP-16RJ45/2RJ45-PM reboots. • If the **Reset/Restore** switch is depressed for greater than approximately 5 seconds it restores the ICDM-RX/TCP-16RJ45/2RJ45-PM to the factory default values.

8.2. Uploading SocketServer to Multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs

You can use this procedure if your ICDM-RX/TCP-16RJ45/2RJ45-PM is connected to the host PC, laptop, or if the ICDM-RX/TCP-16RJ45/2RJ45-PM resides on the local network segment.

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 13) and **Scan** the network.
2. Shift-click the multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs right-click and then click **Advanced > Upload Firmware**.
3. Browse, click the firmware (**.cmtl**) file, **Open** (*Please locate the new firmware*), and then click **Yes** (*Upload Firmware*).

   It may take a few moments for the firmware to upload onto the ICDM-RX/TCP-16RJ45/2RJ45-PM. The ICDM-RX/TCP-16RJ45/2RJ45-PM reboots itself during the upload process.
4. Click **Ok** to the advisory message about waiting to use the device until the status reads **ON-LINE**.

In the next polling cycle, PortVision DX updates and displays the new firmware version. If necessary, you can click **Refresh**.

8.3. Configuring Multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs Network Addresses

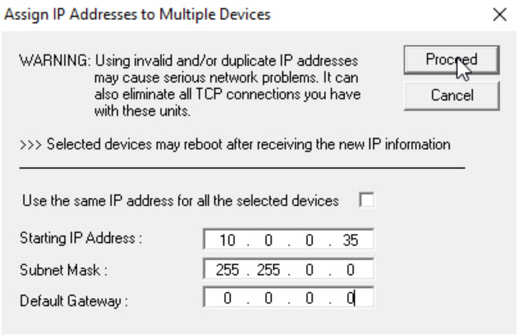
You can configure the network addresses for multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs using the **Assign IP to Multiple Devices** option.

In addition, you can also configure common settings for the ICDM-RX/TCP-16RJ45/2RJ45-PM SocketServer or NS-Link web page and save the settings to a configuration file that you can load to all or selected ICDM-RX/TCP-16RJ45/2RJ45-PMs.

The ICDM-RX/TCP-16RJ45/2RJ45-PMs must be on the same network segment for this procedure to work. Use the following steps to configure multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs.

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 13) and **Scan** the network.
2. Shift-click the ICDM-RX/TCP-16RJ45/2RJ45-PMs for which you want to program network information, right-click, and click **Advanced > Assign IP to Multiple Devices**.
3. Enter the starting IP address, subnet mask, IP Gateway and click **Proceed**.

   PortVision DX displays the programmed IP addresses after the next refresh cycle.


Assign IP Addresses to Multiple Devices

WARNING: Using invalid and/or duplicate IP addresses may cause serious network problems. It can also eliminate all TCP connections you have with these units.

>>> Selected devices may reboot after receiving the new IP information

Use the same IP address for all the selected devices □

Starting IP Address : 10 . 0 . 0 . 35

Subnet Mask : 255 . 255 . 0 . 0

Default Gateway : 0 . 0 . 0 . 0

8.4. Adding a New Device in PortVision DX

You can add a new ICDM-RX/TCP-16RJ45/2RJ45-PM manually, if you do not want to scan the network to locate and add new ICDM-RX/TCP-16RJ45/2RJ45-PMs, but there may be cases where you want to use the *Add New Device* window to:

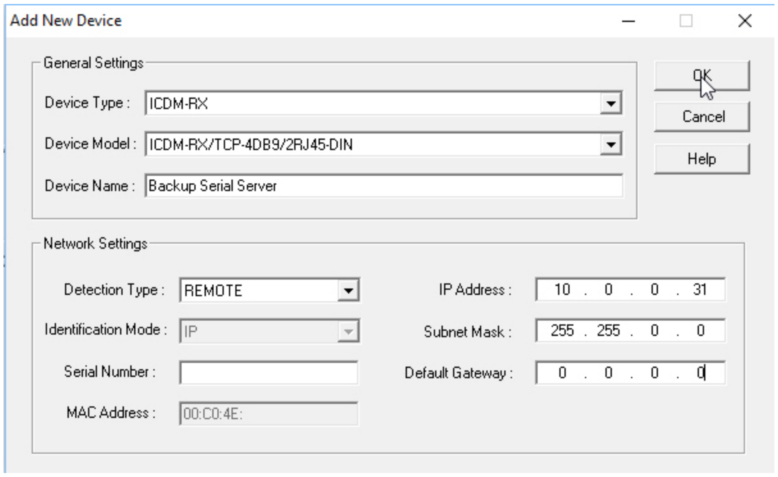
- Configure ICDM-RX/TCP-16RJ45/2RJ45-PM units that are not on the local network (remote) using *Remote Using the IP Address* on Page 68.

- Pre-configure an ICDM-RX/TCP-16RJ45/2RJ45-PM in PortVision DX (local) using *Local Using the IP Address or MAC Address* on Page 69.

8.4.1. Remote Using the IP Address

Use the following procedure to add a remote ICDM-RX/TCP-16RJ45/2RJ45-PM to PortVision DX.

1. Right-click a folder or a RocketLinx switch and click **Add New** > **Device**.
2. Select the appropriate ICDM-RX/TCP-16RJ45/2RJ45-PM in the **Device Type** drop list.
3. Select the appropriate model in the **Device Model** drop list.
4. Enter a friendly device name in the **Device Name** list box.
5. Select **REMOTE** for the *Detection Type*.
6. Optionally, enter the serial number in the **Serial Number** list box.
7. Enter the IP Address for the ICDM-RX/TCP-16RJ45/2RJ45-PM. It is not necessary to enter the Subnet Mask and Default Gateway.



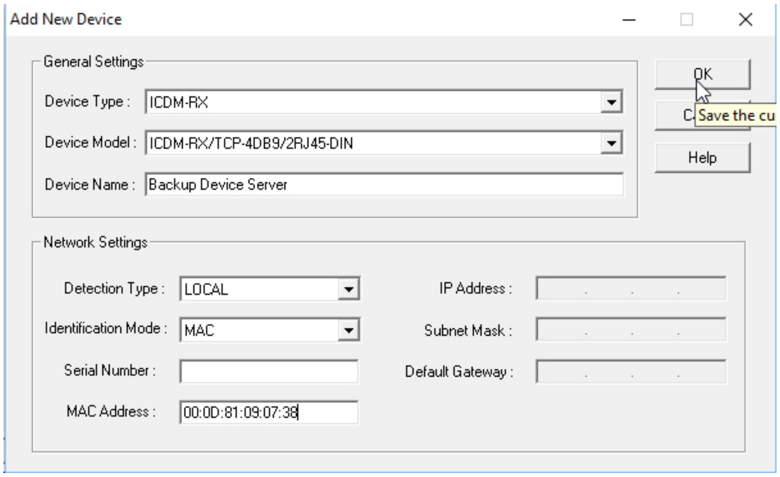
Device Type : ICDM-RX
Device Model : ICDM-RX/TCP-4DB9/2RJ45-DIN
Device Name : Backup Serial Server
Detection Type : REMOTE
Identification Mode : IP
Serial Number :
MAC Address : 00:C0:4E:
IP Address : 10 . 0 . 0 . 31
Subnet Mask : 255 . 255 . 0 . 0
Default Gateway : 0 . 0 . 0 . 0

8. Click **OK** to close the *Add New Device* window. It may take a few moments to save the ICDM-RX/TCP-16RJ45/2RJ45-PM.
9. If necessary, click **Refresh** for the new ICDM-RX/TCP-16RJ45/2RJ45-PM to display. The ICDM-RX/TCP-16RJ45/2RJ45-PM shows OFF-LINE if it is not attached to the network or if an incorrect IP address was entered.

8.4.2. Local Using the IP Address or MAC Address

Use the following procedure to add a local ICDM-RX/TCP-16RJ45/2RJ45-PM to PortVision DX if you do not want to scan the network.

1. Locate the network information or MAC address of the ICDM-RX/TCP-16RJ45/2RJ45-PM you want to add.
2. Right-click a folder or a RocketLinx switch in the *Device Tree* pane (anywhere in the pane, as long as an ICDM-RX/TCP-16RJ45/2RJ45-PM is not highlighted and you are in a valid folder) and click **Add New > Device**.
3. Select the appropriate ICDM-RX/TCP-16RJ45/2RJ45-PM in the **Device Type** drop list.



General Settings

Device Type : ICDM-RX

Device Model : ICDM-RX/TCP-4DB9/2RJ45-DIN

Device Name : Backup Device Server

Network Settings

Detection Type : LOCAL

Identification Mode : MAC

Serial Number :

MAC Address : 00:0D:81:09:07:38

IP Address : . . .

Subnet Mask : . . .

Default Gateway : . . .

4. Select the appropriate model in the **Device Model** drop list.
5. Enter a friendly device name in the **Device Name** list box.
6. Select **LOCAL** for the *Detection Type*.
7. Enter the MAC address or network information.

   Note: *A MAC address label is attached to all ICDM-RX/TCP-16RJ45/2RJ45-PM units.*
8. Optionally, enter the serial number in the **Serial Number** list box.
9. Click **Ok**.
10. If necessary, click **Refresh** for the new ICDM-RX/TCP-16RJ45/2RJ45-PM to display. The ICDM-RX/TCP-16RJ45/2RJ45-PM shows OFF-LINE if it is not attached to the network or if an incorrect IP address was entered.

8.5. Using SocketServer Configuration Files

If you are deploying multiple ICDM-RX/TCP-16RJ45/2RJ45-PM units that share common SocketServer values, you can save and load the configuration file (**.dc**) using either PortVision DX or the web interface.

- *PortVision DX - Saving a SocketServer Configuration File*
- *PortVision DX - Loading a SocketServer Configuration File* on Page 70
- *SocketServer - Saving Configuration Files* on Page 71
- *SocketServer - Loading Configuration Files* on Page 71

If you save a configuration file using PortVision DX, you can choose what settings you want to save or load.

You may want to program the network settings in multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs using *Configuring Multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs Network Addresses* on Page 67.

8.5.1. PortVision DX - Saving a SocketServer Configuration File

Use this procedure to save a configuration file using the PortVision DX **Main** screen.

Note: *Optionally, you can save a configuration file by accessing the* **Software Settings** *tab in the* **Properties** *screen and then clicking the* **Save Settings to a File** *button.*

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 13) and **Scan** the network.
2. Right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM and then click **Configuration** > **Save**.
3. Browse to the location you want to save the file, enter a file name, and click **Save**.
4. Click **OK** to close the *Save Configuration Completed* message.

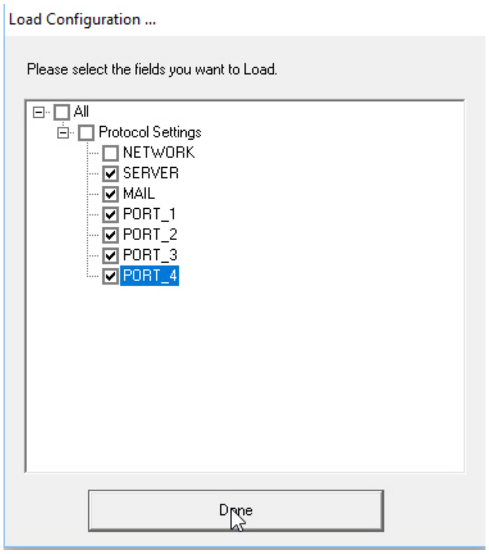
8.5.2. PortVision DX - Loading a SocketServer Configuration File

Use the following procedure to load a previously saved an ICDM-RX/TCP-16RJ45/2RJ45-PM configuration file. Load a configuration file and apply it to a selected ICDM-RX/TCP-16RJ45/2RJ45-PM or ICDM-RX/TCP-16RJ45/2RJ45-PMs.

Use this procedure to load a configuration file one or more ICDM-RX/TCP-16RJ45/2RJ45-PM units.

Note: *The configuration file does not need to be the same model or port density. For example, the saved configuration file could be from an ICDM-RX/TCP-4DB9/2RJ45-DIN that you want to load on an ICDM-RX/TCP-DB9/RJ45-DIN.*

1. Highlight the device or devices, right-click and then click **Configuration** > **Load**
2. Click **Yes** to the warning that it will take 25 seconds per device and it may also reboot the devices.
3. Browse to the location of the configuration file, click the file name (**.dc**) and then **Open**.
4. Click the **All** check box or expand the Protocol Settings and select only the properties that you want to load for each property page in the configuration file and then click **Done**.



Load Configuration ...

Please select the fields you want to Load.

- □ All
  - □ Protocol Settings
    - □ NETWORK
    - ☑ SERVER
    - ☑ MAIL
    - ☑ PORT_1
    - ☑ PORT_2
    - ☑ PORT_3
    - ☑ PORT_4

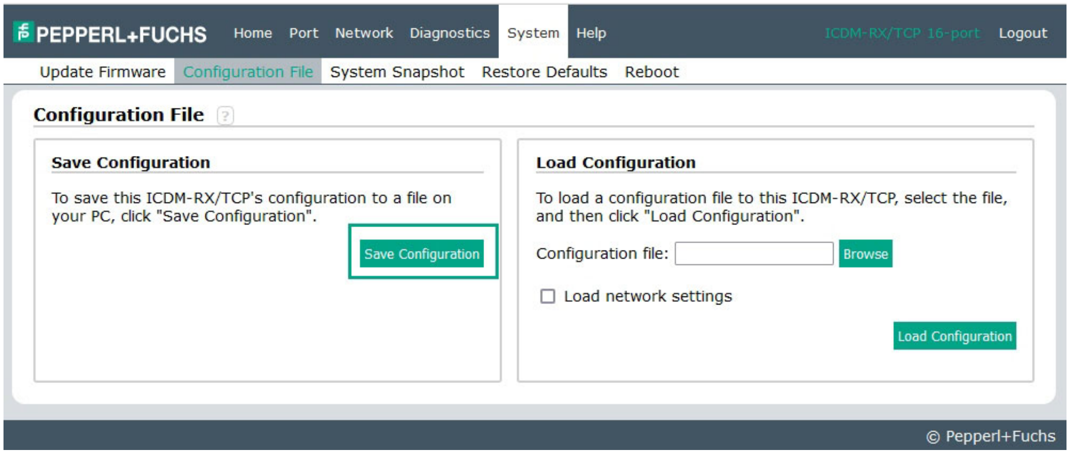
Note: *If you click* **All***, every selected ICDM-RX/TCP-16RJ45/2RJ45-PMs will be programmed with the same IP address.*

5. Close the *Load Configuration* popup message.

8.5.3. SocketServer - Saving Configuration Files

You can use the procedure to save a configuration files using the web page.

1. If necessary, access SocketServer by entering the IP address in your web browser.
2. Click **System | Configuration File**.
3. Click the **Save Configuration** button.



To save this ICDM-RX/TCP's configuration to a file on your PC, click "Save Configuration".

To load a configuration file to this ICDM-RX/TCP, select the file, and then click "Load Configuration".

Configuration file:

□ Load network settings

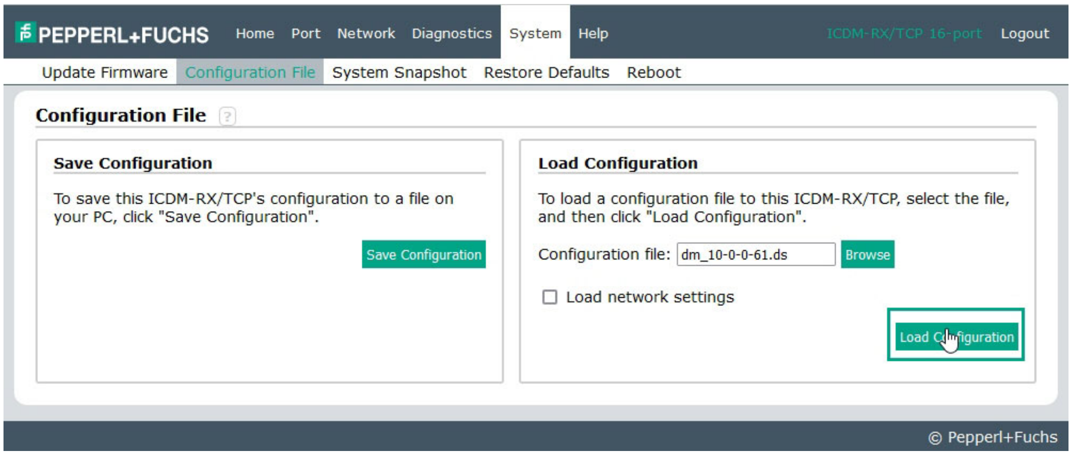
4. Save the configuration file to an appropriate location.

8.5.4. SocketServer - Loading Configuration Files

You can use this procedure to load SocketServer configuration files using SocketServer.

Note: *You must have previously saved a configuration file to load.*

1. If necessary, access SocketServer by entering the IP address in your web browser.
2. Click **System | Configuration File**.
3. Click the **Browse** button, highlight the configuration file, and click the **Open** button.
4. Click the **Load Configuration** button.



To save this ICDM-RX/TCP's configuration to a file on your PC, click "Save Configuration".

To load a configuration file to this ICDM-RX/TCP, select the file, and then click "Load Configuration".

Configuration file: dm_10-0-0-61.ds

□ Load network settings

8.6. Using Driver Configuration Files

This subsection discusses how to create (save) and load driver configuration files. You may want to create driver configuration files for these reasons:

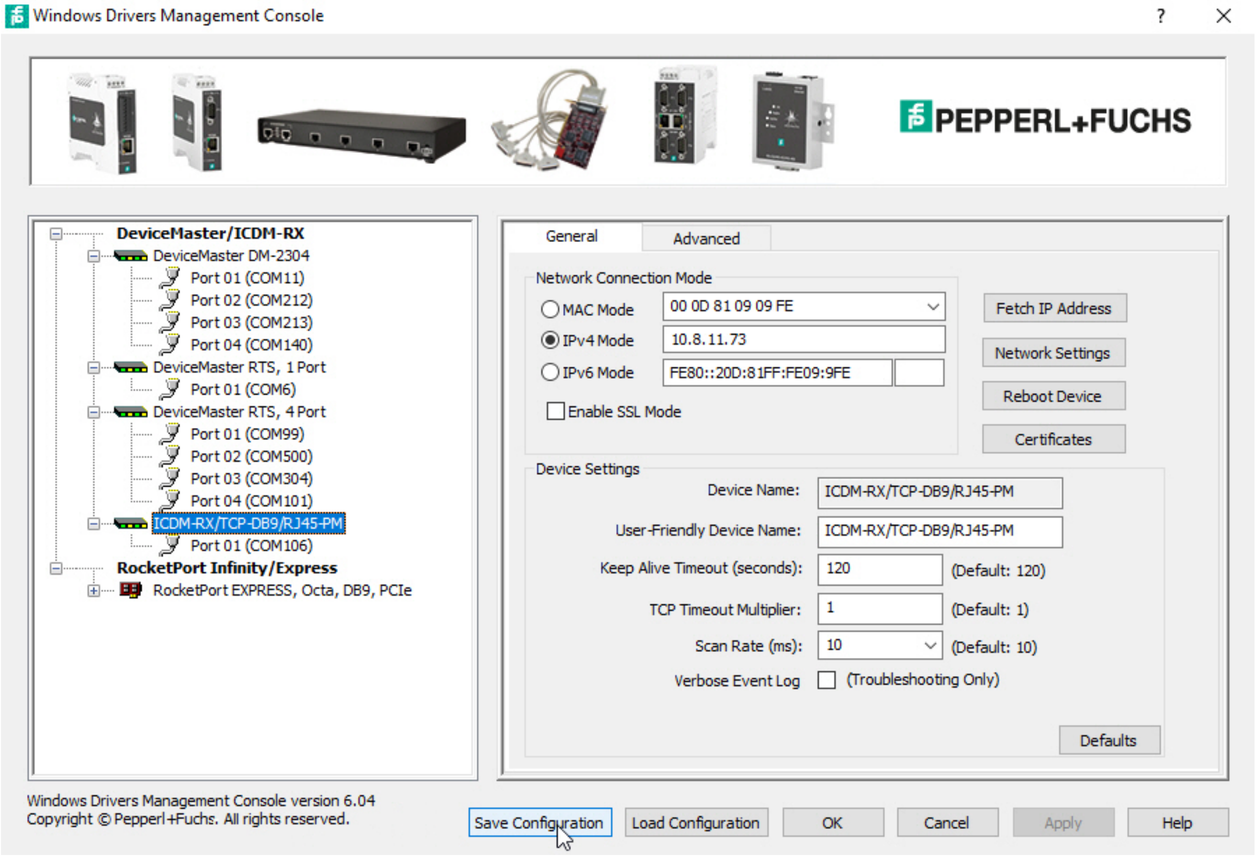
- Save the driver configuration settings so that you can load them on similar ICDM-RX/TCP-16RJ45/2RJ45-PMs to save configuration time
- Save the driver configuration settings because you need to remove a driver version to install a new driver version and you want to reload the driver configuration settings into the new driver

Device driver configuration files must be for the same model with the same port density. For example, you cannot load an ICDM-RX/TCP-DB9/RJ45-DIN (single serial port model) configuration file onto an ICDM-RX/TCP-4DB9/2RJ45-DIN (four serial port model).

8.6.1. Saving Driver Configuration Files

Use the following procedure to create and save a configuration file.

1. If necessary, open the *Windows Drivers Management Console* located under **Pepperl+Fuchs Comtrol>Windows Driver Management Console**.
2. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* User Account Control message.
3. Highlight the ICDM-RX/TCP-16RJ45/2RJ45-PM for which you want to save the driver configuration.
4. Click **Save Configuration**.



DeviceMaster/ICDM-RX
- DeviceMaster DM-2304
  - Port 01 (COM11)
  - Port 02 (COM212)
  - Port 03 (COM213)
  - Port 04 (COM140)
- DeviceMaster RTS, 1 Port
  - Port 01 (COM6)
- DeviceMaster RTS, 4 Port
  - Port 01 (COM99)
  - Port 02 (COM500)
  - Port 03 (COM304)
  - Port 04 (COM101)
- ICDM-RX/TCP-DB9/RJ45-PM
  - Port 01 (COM106)

RocketPort Infinity/Express
- RocketPort EXPRESS, Octa, DB9, PCIe

Network Connection Mode

○ MAC Mode 00 0D 81 09 09 FE
● IPv4 Mode 10.8.11.73
○ IPv6 Mode FE80::20D:81FF:FE09:9FE

☐ Enable SSL Mode

Device Settings

Device Name: ICDM-RX/TCP-DB9/RJ45-PM
User-Friendly Device Name: ICDM-RX/TCP-DB9/RJ45-PM
Keep Alive Timeout (seconds): 120 (Default: 120)
TCP Timeout Multiplier: 1 (Default: 1)
Scan Rate (ms): 10 (Default: 10)
Verbose Event Log ☐ (Troubleshooting Only)

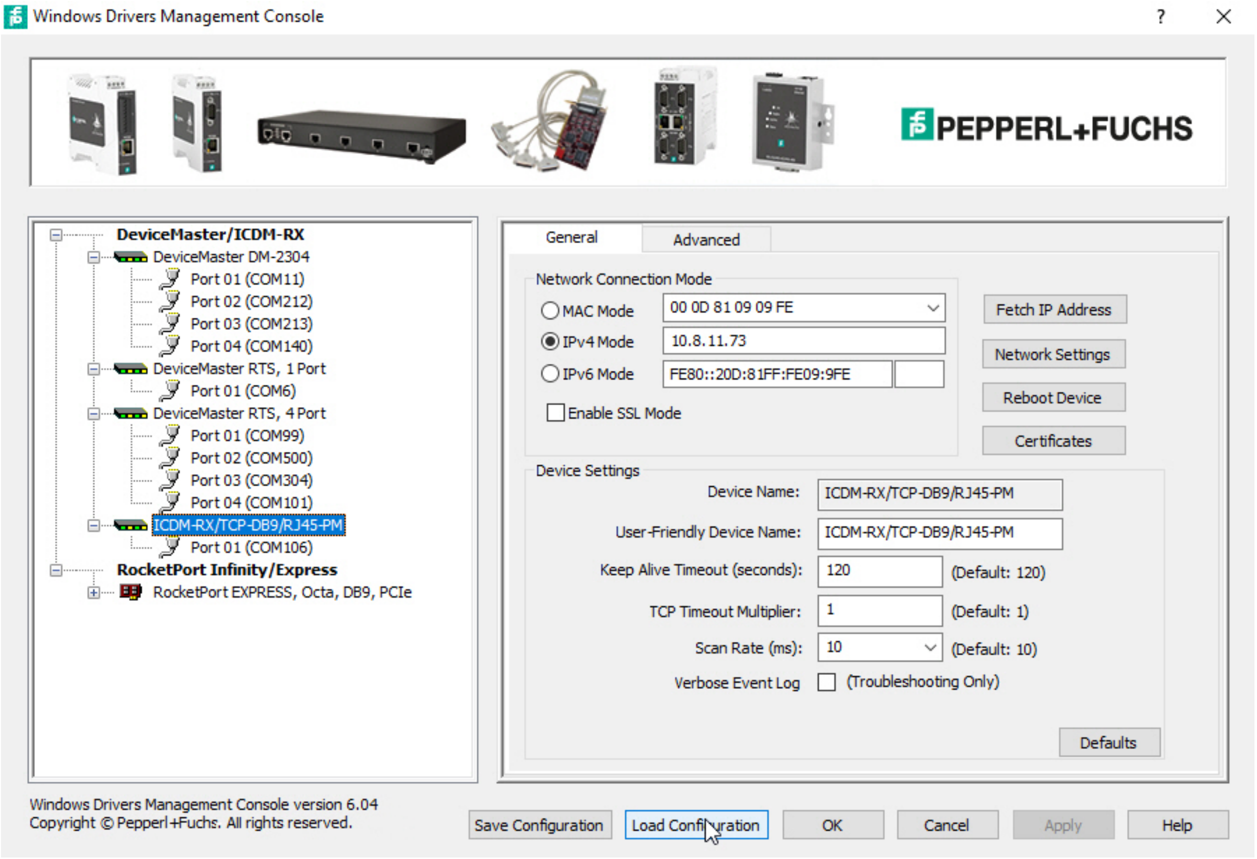
Windows Drivers Management Console version 6.04
Copyright © Pepperl+Fuchs. All rights reserved.

5. If necessary, enter a file name or optionally, change the default file name and click **Save**.
6. Repeat the previous steps for each ICDM-RX/TCP-16RJ45/2RJ45-PM for which you want to save the driver configuration.

8.6.2. Loading Driver Configuration Files

Use the following procedure to load the configuration file for device-level information for your ICDM-RX/TCP-16RJ45/2RJ45-PM.

1. If necessary, open the *Windows Drivers Management Console* located under **Pepperl+Fuchs Comtrol>Windows Driver Management Console**.
2. Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* User Account Control message.
3. In the left pane, highlight the ICDM-RX/TCP-16RJ45/2RJ45-PM for which you want to load the device-level settings from the configuration file.
4. Click **Load Configuration**.



Network Connection Mode

○ MAC Mode 00 0D 81 09 09 FE

● IPv4 Mode 10.8.11.73

○ IPv6 Mode FE80::20D:81FF:FE09:9FE

□ Enable SSL Mode

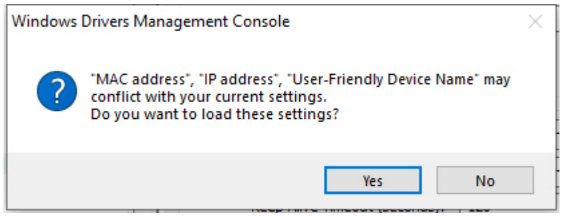
Device Settings

Device Name:	ICDM-RX/TCP-DB9/RJ45-PM	
User-Friendly Device Name:	ICDM-RX/TCP-DB9/RJ45-PM	
Keep Alive Timeout (seconds):	120	(Default: 120)
TCP Timeout Multiplier:	1	(Default: 1)
Scan Rate (ms):	10	(Default: 10)
Verbose Event Log	□	(Troubleshooting Only)

Windows Drivers Management Console version 6.04
Copyright © Pepperl+Fuchs. All rights reserved.

5. Browse to the location of the configuration file that you want to load.
6. Highlight the configuration file and click **Open**. The configuration file loads in a few moments.

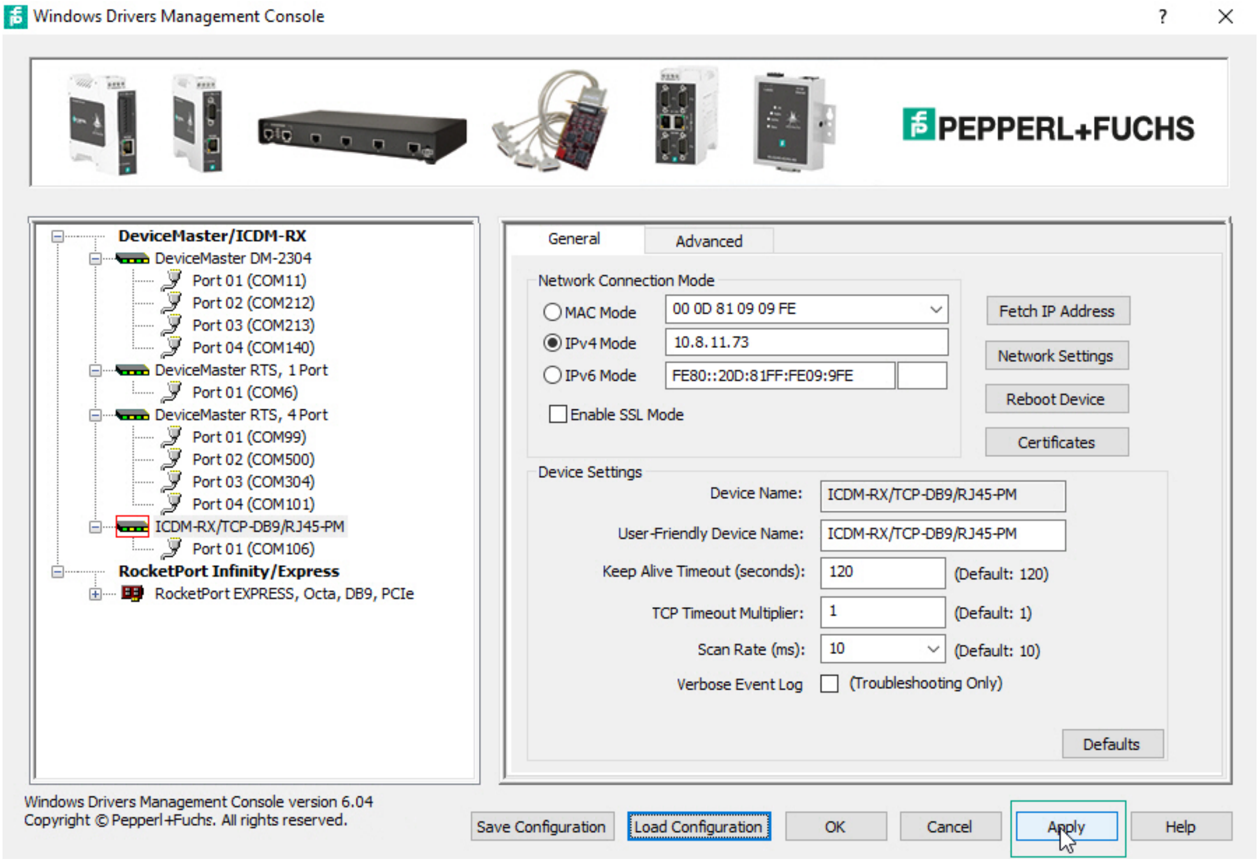
7. Make the appropriate choice for your situation:
   - Click **No** to the message, if you are using the file to set up multiple ICDM-RX/TCP-16RJ45/2RJ45-PMs with the same device-level settings.
   - Click **Yes** to the message, if you are using the file to restore a specific ICDM-RX/TCP-16RJ45/2RJ45-PM. For example, you needed to remove and then re-install the ICDM-RX/TCP-16RJ45/2RJ45-PM NS-Link device driver.



Windows Drivers Management Console

"MAC address", "IP address", "User-Friendly Device Name" may conflict with your current settings.
Do you want to load these settings?

8. Click **Apply** so that the configuration is saved on the ICDM-RX/TCP-16RJ45/2RJ45-PM.



Windows Drivers Management Console

- DeviceMaster/ICDM-RX
  - DeviceMaster DM-2304
    - Port 01 (COM11)
    - Port 02 (COM212)
    - Port 03 (COM213)
    - Port 04 (COM140)
  - DeviceMaster RTS, 1 Port
    - Port 01 (COM6)
  - DeviceMaster RTS, 4 Port
    - Port 01 (COM99)
    - Port 02 (COM500)
    - Port 03 (COM304)
    - Port 04 (COM101)
  - ICDM-RX/TCP-DB9/RJ45-PM
    - Port 01 (COM106)
- RocketPort Infinity/Express
  - RocketPort EXPRESS, Octa, DB9, PCIe

Network Connection Mode

○ MAC Mode 00 0D 81 09 09 FE
● IPv4 Mode 10.8.11.73
○ IPv6 Mode FE80::20D:81FF:FE09:9FE
□ Enable SSL Mode

Device Settings

Device Name: ICDM-RX/TCP-DB9/RJ45-PM
User-Friendly Device Name: ICDM-RX/TCP-DB9/RJ45-PM
Keep Alive Timeout (seconds): 120 (Default: 120)
TCP Timeout Multiplier: 1 (Default: 1)
Scan Rate (ms): 10 (Default: 10)
Verbose Event Log □ (Troubleshooting Only)

Windows Drivers Management Console version 6.04
Copyright © Pepperl+Fuchs. All rights reserved.

8.7. Changing the Bootloader Timeout

If SocketServer fails during the upload process, you should change the **Bootloader timeout** value to 45 seconds.

Note: *The ICDM-RX/TCP-16RJ45/2RJ45-PM must be able to communicate using an IP address, which is compatible with this local network. If necessary, refer to Configuring the Network Settings (PortVision DX) on Page 14.*

8.7.1. PortVision DX - Changing Bootloader Timeout

Use the following procedure to change the Bootloader timeout to 45 seconds. You can use this procedure to return the Bootloader timeout to 15 seconds after you have successfully uploaded SocketServer.

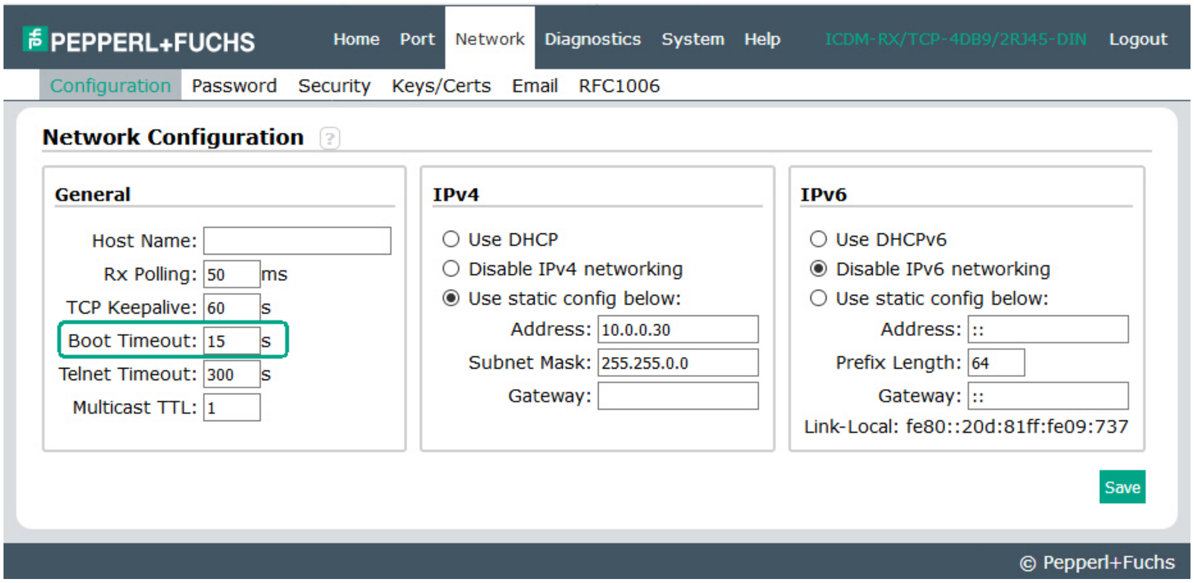
1. If necessary, start PortVision DX, from **Pepperl+Fuchs Comtrol** > **PortVision DX**.
2. Right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM and click **Properties**.
3. Type 45 in the **Bootloader Timeout** text box and click **Apply**.

Note: *You should return the Bootloader Timeout value back to 15 seconds after you upload SocketServer.*

8.7.2. SocketServer - Changing Bootloader Timeout

Use the following procedure to change the Bootloader timeout to 45 seconds. You can use this procedure to return the Bootloader timeout to 15 seconds after you have successfully uploaded SocketServer.

1. If necessary, use your browser to access the ICDM-RX/TCP-16RJ45/2RJ45-PM using the IP address.
2. Click **Network**.
3. Enter 45 in the **Boot Timeout** field and click **Save**.



Network Configuration

General

Host Name:
Rx Polling: 50 ms
TCP Keepalive: 60 s
Boot Timeout: 15 s
Telnet Timeout: 300 s
Multicast TTL: 1

IPv4

○ Use DHCP
○ Disable IPv4 networking
● Use static config below:
Address: 10.0.0.30
Subnet Mask: 255.255.0.0
Gateway:

IPv6

○ Use DHCPv6
● Disable IPv6 networking
○ Use static config below:
Address: ::
Prefix Length: 64
Gateway: ::
Link-Local: fe80::20d:81ff:fe09:737

Note: *You should return the Bootloader Timeout value back to 15 seconds after you upload the firmware.*

8.8. Using Configuration Files

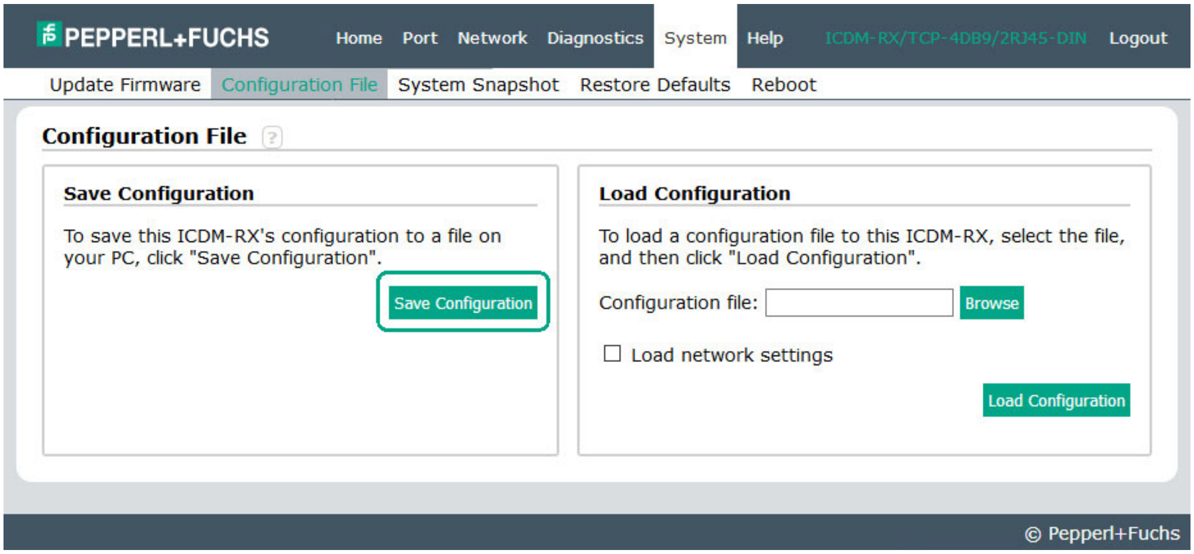
This subsection discusses how to create (save) and load ICDM-RX/TCP-16RJ45/2RJ45-PM configuration files. You may want to create ICDM-RX/TCP-16RJ45/2RJ45-PM configuration files for these reasons:

- Save the ICDM-RX/TCP-16RJ45/2RJ45-PM configuration settings so that you can load them on similar ICDM-RX/TCP-16RJ45/2RJ45-PMs to save configuration ICDM-RX/TCP-16RJ45/2RJ45-PM
- Save the ICDM-RX/TCP-16RJ45/2RJ45-PM configuration settings because you need to remove a firmware version to install a new firmware version and you want to reload the configuration settings into the new firmware.

8.8.1. Saving Configuration Files

Use this procedure to save configuration files.

1. Enter the IP address into your browser to access the web interface.
2. Click **System | Configuration File**.
3. Click the **Save Configuration** button.



Configuration File

Save Configuration

To save this ICDM-RX's configuration to a file on your PC, click "Save Configuration".

Load Configuration

To load a configuration file to this ICDM-RX, select the file, and then click "Load Configuration".

Configuration file:

☐ Load network settings

4. Depending on your browser, may need to click save or direct it to a specific file location.

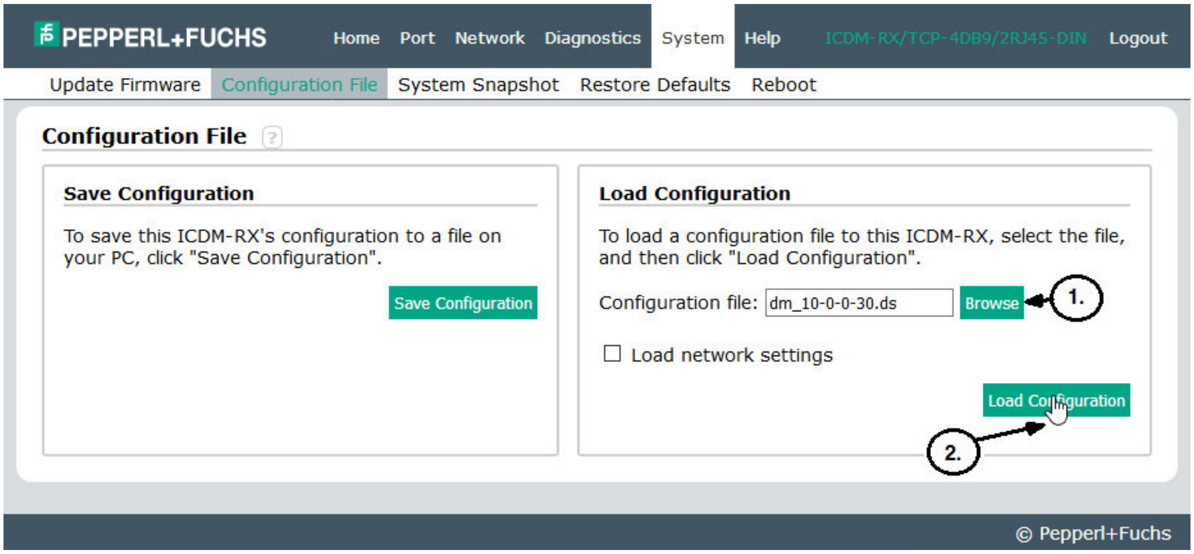
8.8.2. Loading Configuration Files

Use the following procedure to load configuration files.

1. If necessary, enter the IP address in your browser.
2. Click **System | Configuration File**.
3. Click the **Browse** button and select the configuration file. The default configuration file name is:

   dm_xxx.xxx.xxx.xxx.ds

   Where *xxx.xxx.xxx.xxx* is the IP address and *.ds* is the file extension.
4. Click the **Load Configuration** button.



Configuration File

Save Configuration

To save this ICDM-RX's configuration to a file on your PC, click "Save Configuration".

Load Configuration

To load a configuration file to this ICDM-RX, select the file, and then click "Load Configuration".

Configuration file: dm_10-0-0-30.ds

☐ Load network settings

8.9. Managing Bootloader

Bootloader refers to the operating system that runs on the ICDM-RX/TCP-16RJ45/2RJ45-PM hardware during the power on phase, which then loads SocketServer.

Note: *Typically, you should not update the Bootloader unless advised to do so by Pepperl+Fuchs Technical Support.*

There are several methods and tools that you can use to check the Bootloader version or update the Bootloader.

- **PortVision DX** is the easiest way to check the Bootloader version and upload the latest version.
- Optionally, RedBoot can be used to check the Bootloader version and update the Bootloader. See *RedBoot Procedures* on Page 88 for procedures.

8.9.1. Checking the Bootloader Version

The following procedure uses PortVision DX to check the Bootloader version. Optionally, you can use RedBoot, see *Determining the Bootloader Version* on Page 92.

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 13) and **Scan** the network.
2. Right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM and click **Advanced** > **Reboot**.

3. Click **Yes** to the *Confirm Reboot* query.
4. Right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM, click **Refresh.** You may need to do this several times until you catch the reboot cycle. The Bootloader version is briefly displayed during the reboot cycle before SocketServer application loads.
5. Check the **https://www.pepperl-fuchs.com** web site to see if a later version of Bootloader is available.
6. Go to the next subsection if you need upload a new version of Bootloader.

8.9.2. Uploading Bootloader

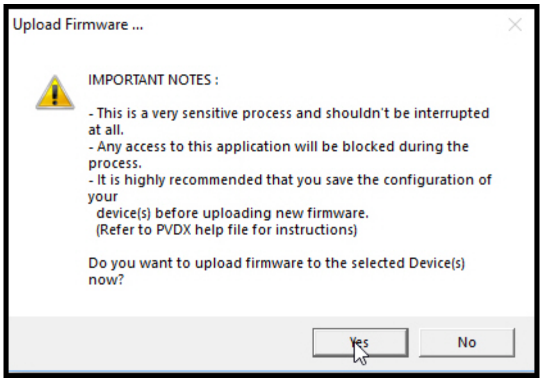
Use the following procedure to upload Bootloader to the ICDM-RX/TCP-16RJ45/2RJ45-PM. Typically, you should not update the Bootloader unless advised to do so by Pepperl+Fuchs Technical Support or a notice has been posted with the firmware at https://www.pepperl-fuchs.com.

Note: *Technical Support does not recommend updating Bootloader across a WAN. For best results, connect the ICDM-RX/TCP-16RJ45/2RJ45-PM directly to a PC or laptop to upload Bootloader.*

⚠ ***Make sure that power is not interrupted while uploading Bootloader. Power interruption while uploading Bootloader will require that the ICDM-RX/TCP-16RJ45/2RJ45-PM must be sent into Pepperl+Fuchs so that it can be reflashed.***

If you are not successful uploading SocketServer into the ICDM-RX/TCP-16RJ45/2RJ45-PM, do not upload Bootloader.

1. If you have not done so, install PortVision DX (*Installing PortVision DX* on Page 13) and **Scan** the network.
2. If necessary, check the Bootloader version (*Checking the Bootloader Version* on Page 77) and download the latest version.
3. Right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM for which you want to update, click **Advanced > Upload Firmware**, browse to the Bootloader **.cmtl** file, and then click **Open**.
4. Click **Yes** to the *Upload Firmware* message that warns you that this is a sensitive process.



Upload Firmware ...

IMPORTANT NOTES :

- This is a very sensitive process and shouldn't be interrupted at all.
- Any access to this application will be blocked during the process.
- It is highly recommended that you save the configuration of your
  device(s) before uploading new firmware.
  (Refer to PVDX help file for instructions)

Do you want to upload firmware to the selected Device(s) now?

5. Click **OK** to the second *Upload Firmware* message.
6. Right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM and click **Refresh** until the Bootloader version displays and verify that the new version loaded.

8.10. Checking the NS-Link Version

Use this procedure to check the NS-Link web page version. Remember, an NS-Link version displays when the NS-Link device driver has been installed and configured, NS-Link is the same firmware as SocketServer.

1. Start PortVision DX.
2. If necessary, click **Scan** to locate the ICDM-RX/TCP-16RJ45/2RJ45-PM.
3. Contact Technical Support at https://www.pepperl-fuchs.com to see if a later version of SocketServer is available.

   To check the NS-Link version, you will need to check to see what version of SocketServer is available.
4. Compare the version number displayed in PortVision DX to the version displayed on the web site.
5. If a higher version of SocketServer is available and you want to update the ICDM-RX/TCP-16RJ45/2RJ45-PM with the latest software:
   a. Update SocketServer using *Uploading SocketServer with PortVision DX* on Page 16.
   b. Download the latest driver from the Pepperl+Fuchs web site.
   c. Upload SocketServer to the ICDM-RX/TCP-16RJ45/2RJ45-PM using PortVision DX or the SocketServer web page.

8.11. Restoring Serial Port Settings

Use the web page and/or the NS-Link device driver for Windows to restore the serial port settings to their default values.

The NS-Link serial port settings are independent of the socket serial port settings on the web page. If you are using COM ports and also have configured the port for socket services, you must restore the default port settings in the driver and web page.

8.11.1.NS-Link COM Port

You can use this procedure to reset NS-Link serial port settings.

1. Open the *Windows Drivers Management Console* using **Pepperl+Fuchs Comtrol>Windows Driver Management Console**
2. Highlight the first port that you want reset to default values.
3. Click the **Defaults** button (and if appropriate, **Clone**).
4. Click **Apply** or **OK**.

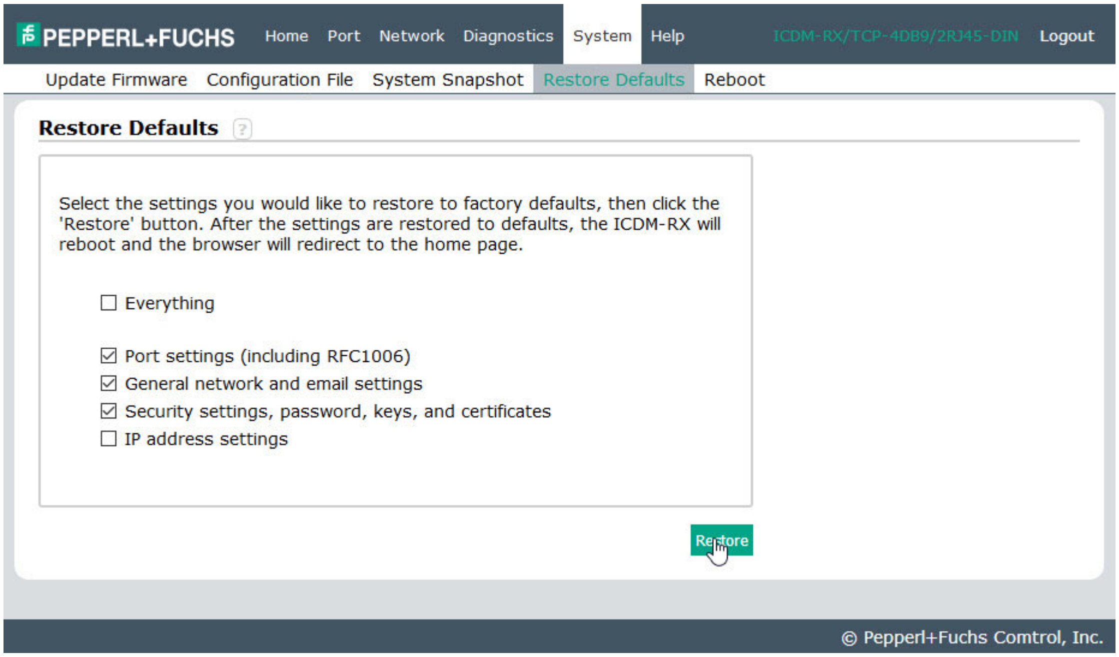
If necessary, you can reset ICDM-RX/TCP-16RJ45/2RJ45-PM device properties to their defaults on the *Device General* tab using the **Defaults** button.

8.11.2.Socket Port

Use the following procedure to reset the socket port serial settings.

1. Open the ICDM-RX/TCP-16RJ45/2RJ45-PM web page (*Accessing Socket Configuration* on Page 32).
2. Click **System | Restore Defaults**.

3. Click the **Port Settings (including RFC1006)** option and then click **Restore**.



Restore Defaults

Select the settings you would like to restore to factory defaults, then click the 'Restore' button. After the settings are restored to defaults, the ICDM-RX will reboot and the browser will redirect to the home page.

- ☐ Everything
- ☑ Port settings (including RFC1006)
- ☑ General network and email settings
- ☑ Security settings, password, keys, and certificates
- ☐ IP address settings

You will be able to log in after the reboot cycle.

8.12. Accessing SocketServer Commands in Telnet/SSH Sessions (PortVision DX)

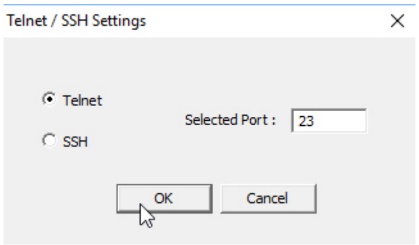
You can open a Telnet or SSH session using PortVision DX. Use the appropriate procedure for your site:

- *Telnet Session* (below)
- *SSH Session* on Page 82

8.12.1.Telnet Session

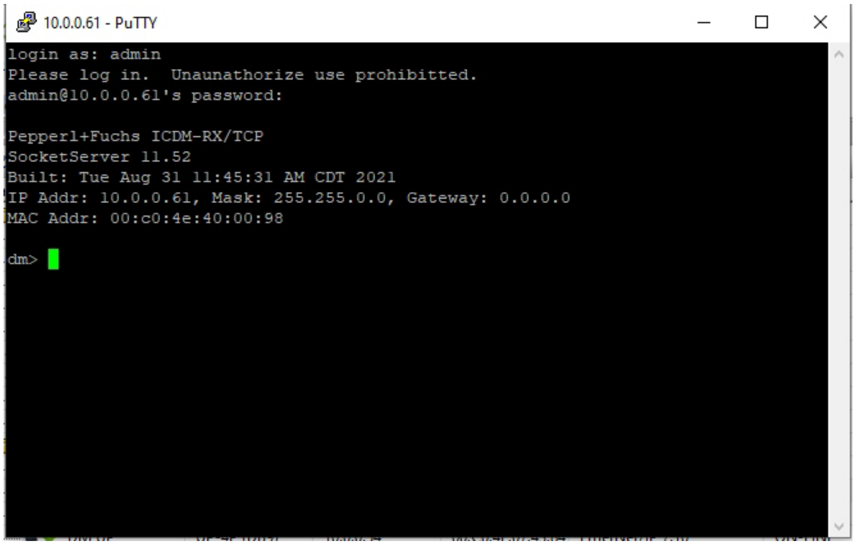
Use the following procedure to access a telnet session with PortVision DX.

1. In PortVision DX, PortVision DX, right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM for which you want to open a telnet session, and click **Telnet/SSH Session**.
2. Leave the popup set to **Telnet** and **Selected Port 23**, and click **OK**



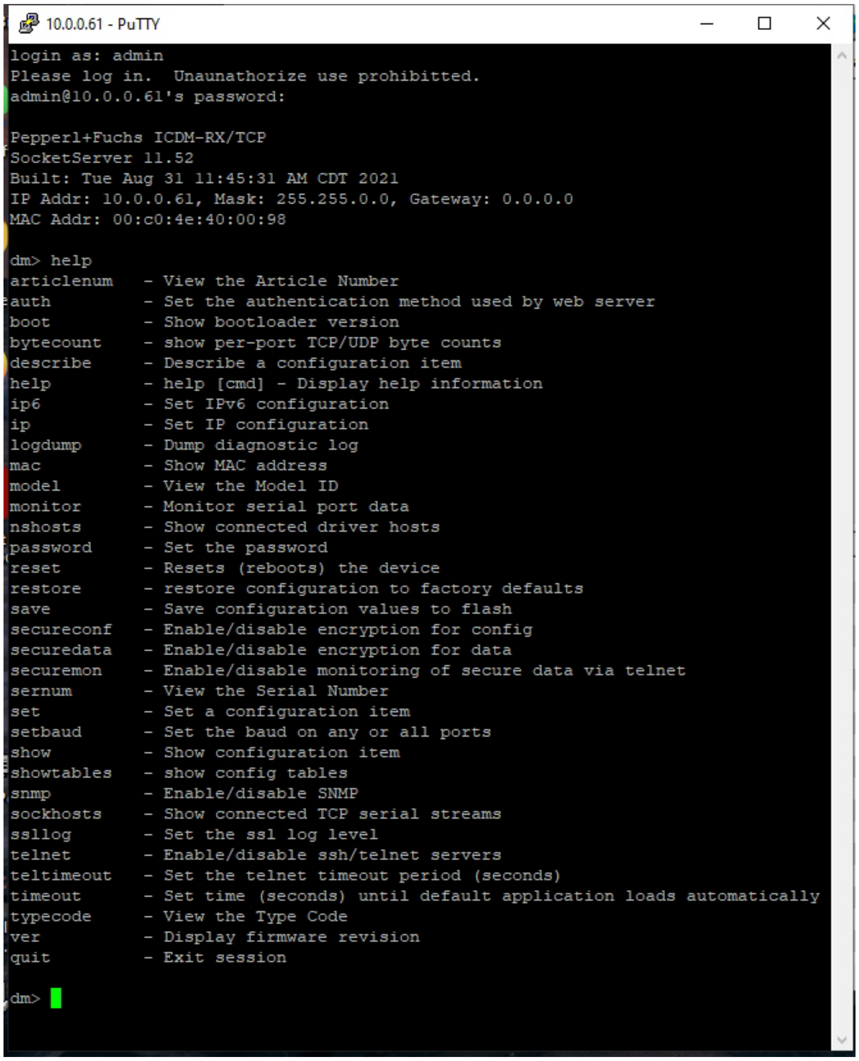
● Telnet
○ SSH
Selected Port : 23

3. If necessary, enter the password and press **Enter**. If a password has not been set, press **Enter**.



```
login as: admin
Please log in.  Unaunathorize use prohibitted.
admin@10.0.0.61's password:

Pepperl+Fuchs ICDM-RX/TCP
SocketServer 11.52
Built: Tue Aug 31 11:45:31 AM CDT 2021
IP Addr: 10.0.0.61, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:c0:4e:40:00:98

dm>
```

4. You can type **help** to refer to available commands supported by SocketServer/NS-Link.

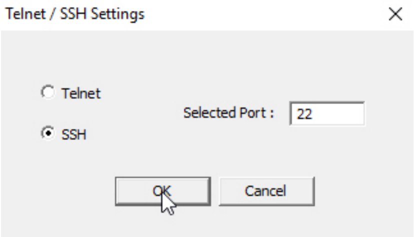


```
login as: admin
Please log in.  Unaunathorize use prohibited.
admin@10.0.0.61's password:

Pepperl+Fuchs ICDM-RX/TCP
SocketServer 11.52
Built: Tue Aug 31 11:45:31 AM CDT 2021
IP Addr: 10.0.0.61, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:c0:4e:40:00:98

dm> help
articlenum     - View the Article Number
auth           - Set the authentication method used by web server
boot           - Show bootloader version
bytecount      - show per-port TCP/UDP byte counts
describe       - Describe a configuration item
help           - help [cmd] - Display help information
ip6            - Set IPv6 configuration
ip             - Set IP configuration
logdump        - Dump diagnostic log
mac            - Show MAC address
model          - View the Model ID
monitor        - Monitor serial port data
nshosts        - Show connected driver hosts
password       - Set the password
reset          - Resets (reboots) the device
restore        - restore configuration to factory defaults
save           - Save configuration values to flash
secureconf     - Enable/disable encryption for config
securedata     - Enable/disable encryption for data
securemon      - Enable/disable monitoring of secure data via telnet
sernum         - View the Serial Number
set            - Set a configuration item
setbaud        - Set the baud on any or all ports
show           - Show configuration item
showtables     - show config tables
snmp           - Enable/disable SNMP
sockhosts      - Show connected TCP serial streams
ssllog         - Set the ssl log level
telnet         - Enable/disable ssh/telnet servers
teltimeout     - Set the telnet timeout period (seconds)
timeout        - Set time (seconds) until default application loads automatically
typecode       - View the Type Code
ver            - Display firmware revision
quit           - Exit session

dm>
```

8.12.2.SSH Session

Use the following procedure to access an SSH session with PortVision DX.

1. In PortVision DX, PortVision DX, right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM for which you want to open an SSH session, and click **Telnet/SSH Session**.
2. Click **SSH** and leave the port number at the default.

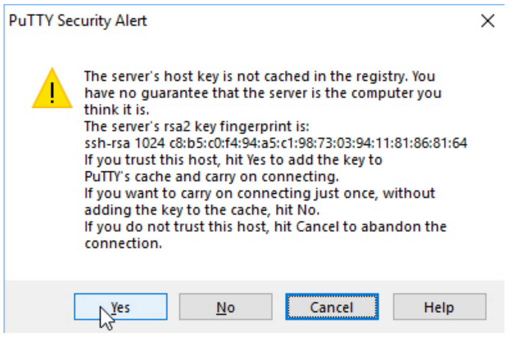


○ Telnet

● SSH

Selected Port : 22

3. If necessary (depending on the operating system), respond to the security notification.



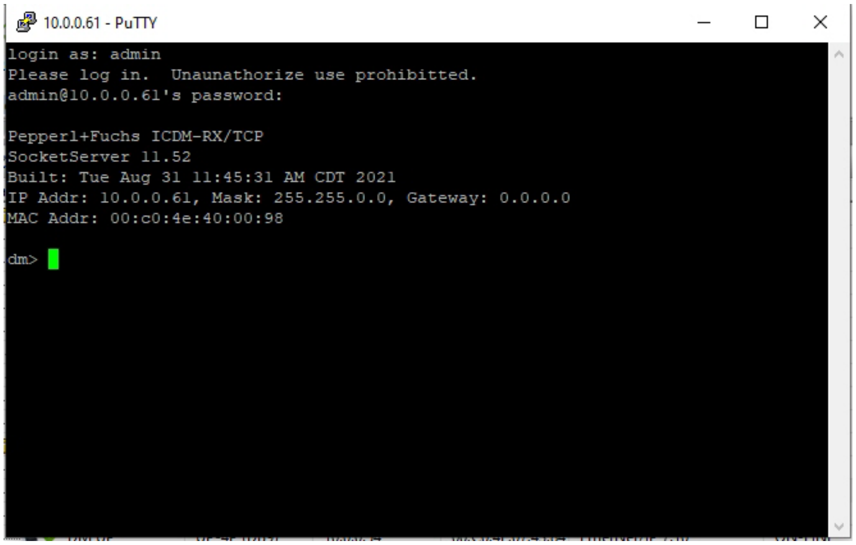
PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 c8:b5:c0:f4:94:a5:c1:98:73:03:94:11:81:86:81:64
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

4. Enter **admin** for the login as name and press **Enter**.

   Note: *The ICDM-RX/TCP-16RJ45/2RJ45-PM requires* ***admin*** *as the login name.*

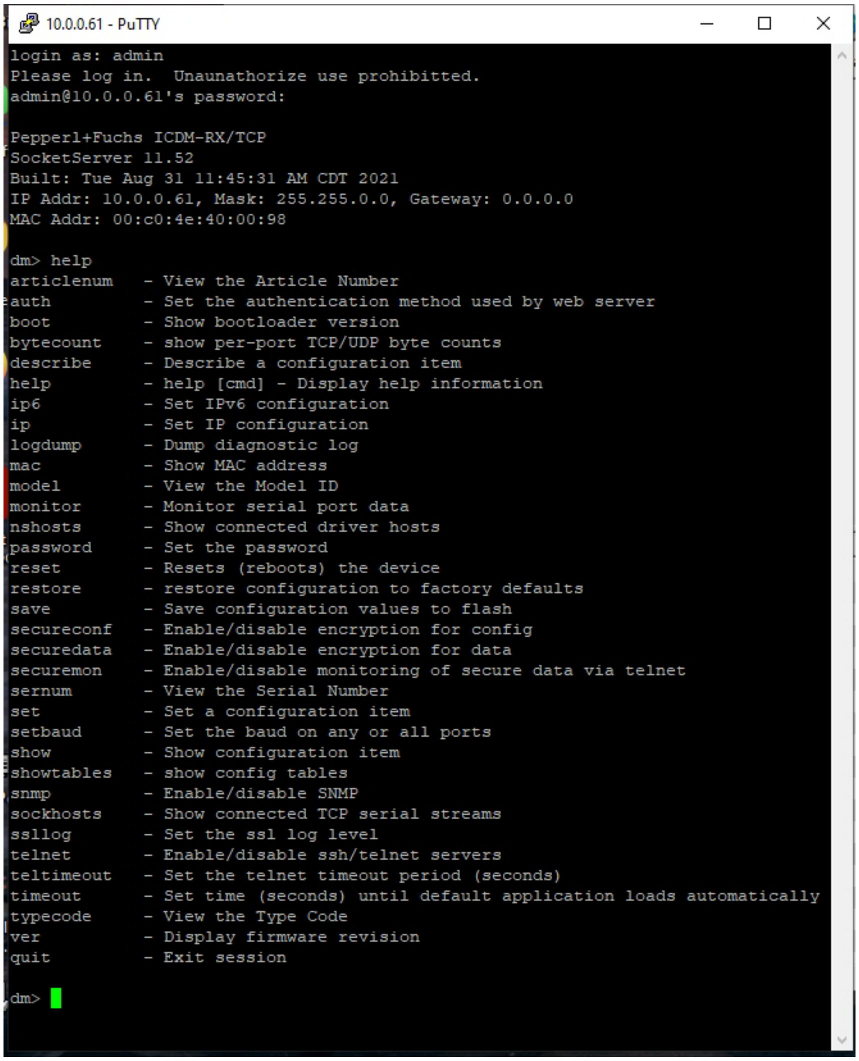
5. If necessary, enter the password and press **Enter**. If a password has not been set, press **Enter**.



10.0.0.61 - PuTTY

```
login as: admin
Please log in.  Unaunathorize use prohibitted.
admin@10.0.0.61's password:

Pepperl+Fuchs ICDM-RX/TCP
SocketServer 11.52
Built: Tue Aug 31 11:45:31 AM CDT 2021
IP Addr: 10.0.0.61, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:c0:4e:40:00:98

dm>
```

6. You can type **help** to refer to available SocketServer/NS-Link commands.



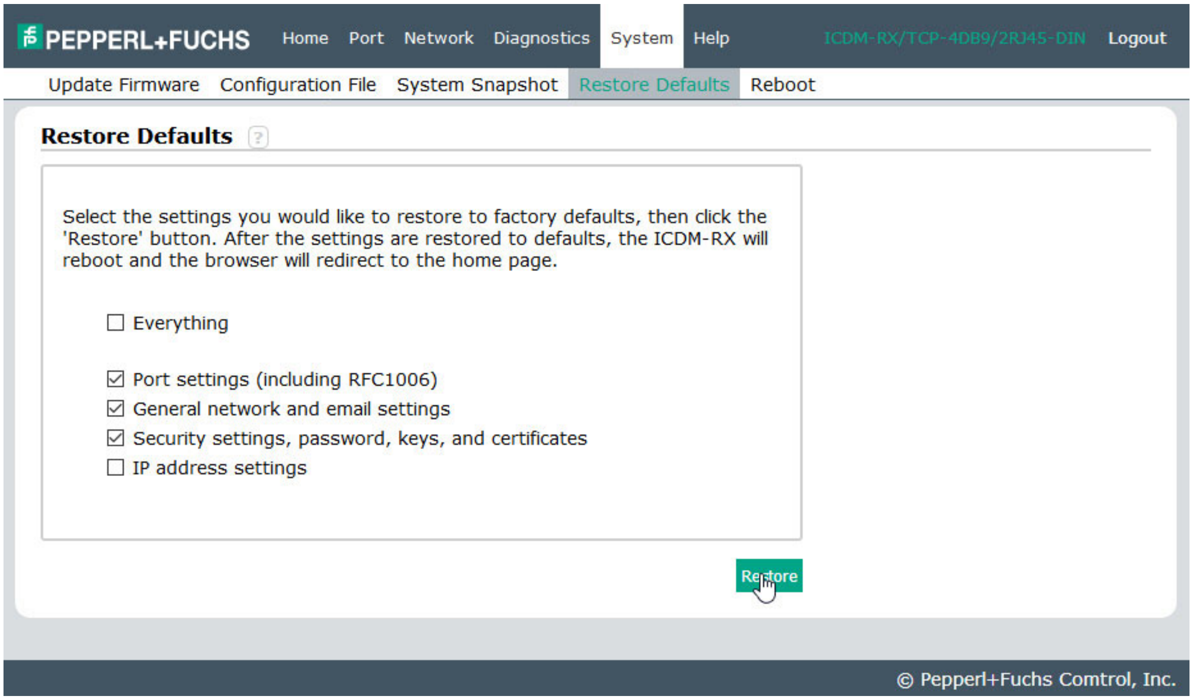
```
login as: admin
Please log in.  Unaunathorize use prohibited.
admin@10.0.0.61's password:

Pepperl+Fuchs ICDM-RX/TCP
SocketServer 11.52
Built: Tue Aug 31 11:45:31 AM CDT 2021
IP Addr: 10.0.0.61, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:c0:4e:40:00:98

dm> help
articlenum    - View the Article Number
auth          - Set the authentication method used by web server
boot          - Show bootloader version
bytecount     - show per-port TCP/UDP byte counts
describe      - Describe a configuration item
help          - help [cmd] - Display help information
ip6           - Set IPv6 configuration
ip            - Set IP configuration
logdump       - Dump diagnostic log
mac           - Show MAC address
model         - View the Model ID
monitor       - Monitor serial port data
nshosts       - Show connected driver hosts
password      - Set the password
reset         - Resets (reboots) the device
restore       - restore configuration to factory defaults
save          - Save configuration values to flash
secureconf    - Enable/disable encryption for config
securedata    - Enable/disable encryption for data
securemon     - Enable/disable monitoring of secure data via telnet
sernum        - View the Serial Number
set           - Set a configuration item
setbaud       - Set the baud on any or all ports
show          - Show configuration item
showtables    - show config tables
snmp          - Enable/disable SNMP
sockhosts     - Show connected TCP serial streams
ssllog        - Set the ssl log level
telnet        - Enable/disable ssh/telnet servers
teltimeout    - Set the telnet timeout period (seconds)
timeout       - Set time (seconds) until default application loads automatically
typecode      - View the Type Code
ver           - Display firmware revision
quit          - Exit session

dm>
```

8.13. Restoring Defaults

Use the following procedure to return some or all of the ICDM-RX/TCP-16RJ45/2RJ45-PM settings to factory default values.

1. Open the web interface bye entering the IP address in your browser.
2. Click **System | Restore Defaults**.
3. Select the items that you want to restore to factory defaults.

4. Click the **Restore** button.


PEPPERL+FUCHS
Home Port Network Diagnostics System Help
ICDM-RX/TCP-4DB9/2RJ45-DIN
Logout
Update Firmware Configuration File System Snapshot Restore Defaults Reboot
Restore Defaults
?

Select the settings you would like to restore to factory defaults, then click the 'Restore' button. After the settings are restored to defaults, the ICDM-RX will reboot and the browser will redirect to the home page.

☐ Everything

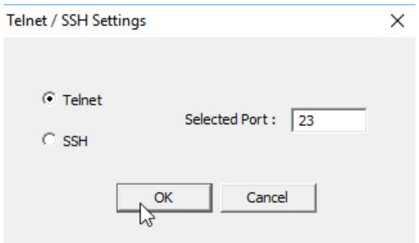
☑ Port settings (including RFC1006)
☑ General network and email settings
☑ Security settings, password, keys, and certificates
☐ IP address settings

8.14. Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)

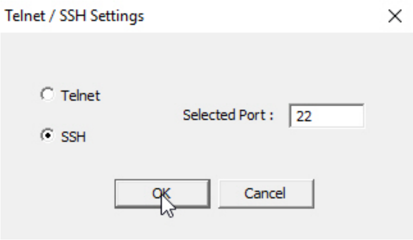
You can open a Telnet or SSH session using PortVision DX to access RedBoot commands.

Use the following procedure to access a telnet or SSH session with PortVision DX.

1. In PortVision DX, PortVision DX, right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM for which you want to open a telnet session, and click **Telnet/SSH Session**.
2. Select **Telnet** or **SSH**, leave the **Selected Port** number, and click **OK**

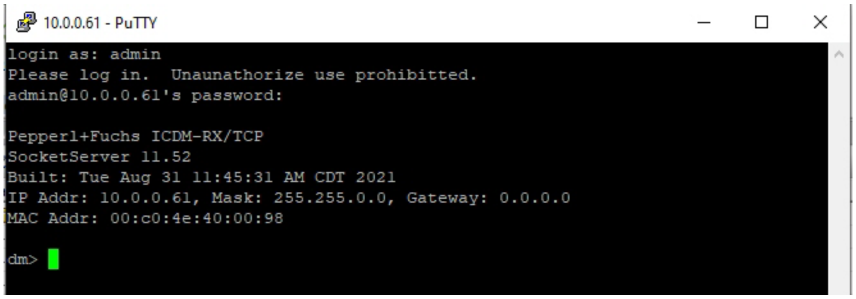


● Telnet
○ SSH
Selected Port : 23



○ Telnet
● SSH
Selected Port : 22

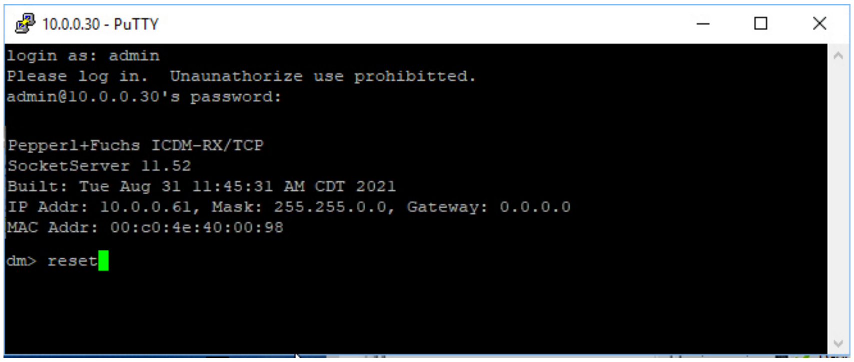
3. If necessary, enter the password and press **Enter**. If a password has not been set, press **Enter**. If using an SSH session, enter **admin** as the login and press **Enter.**



```
login as: admin
Please log in.  Unaunathorize use prohibitted.
admin@10.0.0.61's password:

Pepperl+Fuchs ICDM-RX/TCP
SocketServer 11.52
Built: Tue Aug 31 11:45:31 AM CDT 2021
IP Addr: 10.0.0.61, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:c0:4e:40:00:98

dm>
```

If the PuTTY screen flashes in the background and does not appear as shown above, make sure that **Enable Telnet/ssh** has not been disabled in the web page. To check this, return to PortVision DX, right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM, and click **Webpage**. Click the **Network | Security** and verify that the **Enable Telnet/ssh** option is enabled, If it is not, click the option and then click **Save**, and close the web interface.

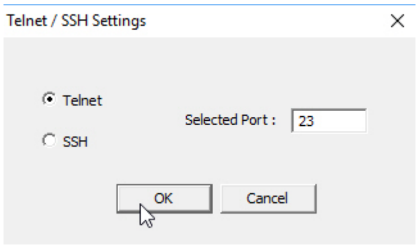
4. Type **Reset**, press **Enter**, and close the telnet session.



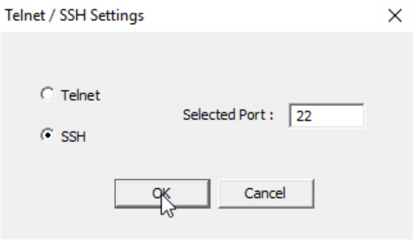
```
login as: admin
Please log in.  Unaunathorize use prohibitted.
admin@10.0.0.30's password:

Pepperl+Fuchs ICDM-RX/TCP
SocketServer 11.52
Built: Tue Aug 31 11:45:31 AM CDT 2021
IP Addr: 10.0.0.61, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:c0:4e:40:00:98

dm> reset
```

5. Quickly re-open the telnet or SSH session using the previous steps.

6. Select **Telnet** or **SSH**, leave the **Selected Port** number, and click **OK**

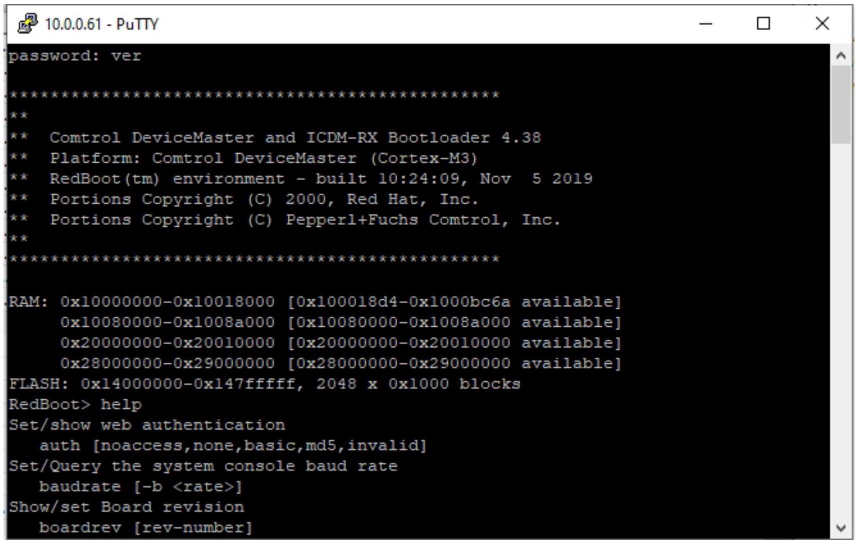


● Telnet
○ SSH
Selected Port : 23



○ Telnet
● SSH
Selected Port : 22

7. Press **Enter**. You can type **help** to review the RedBoot commands. You can also refer to *RedBoot Command Overview* on Page 94.



```
password: ver

************************************************
**
**   Comtrol DeviceMaster and ICDM-RX Bootloader 4.38
**   Platform: Comtrol DeviceMaster (Cortex-M3)
**   RedBoot(tm) environment - built 10:24:09, Nov  5 2019
**   Portions Copyright (C) 2000, Red Hat, Inc.
**   Portions Copyright (C) Pepperl+Fuchs Comtrol, Inc.
**
************************************************

RAM: 0x10000000-0x10018000 [0x100018d4-0x1000bc6a available]
     0x10080000-0x1008a000 [0x10080000-0x1008a000 available]
     0x20000000-0x20010000 [0x20000000-0x20010000 available]
     0x28000000-0x29000000 [0x28000000-0x29000000 available]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks
RedBoot> help
Set/show web authentication
   auth [noaccess,none,basic,md5,invalid]
Set/Query the system console baud rate
   baudrate [-b <rate>]
Show/set Board revision
   boardrev [rev-number]
```

Note: *The dm prompt should be replaced by a Redboot prompt. If not, you can reset the Bootloader timeout for a longer time period and retry this procedure.*

9. RedBoot Procedures

You can use this section as a reference if you want to perform tasks in RedBoot.

- *Accessing RedBoot Overview* on Page 88
- *Establishing a Serial Connection* on Page 89
- *Establishing a Telnet Connection* on Page 90
- *Determining the Network Settings* on Page 91
- *Configuring the Network Settings* on Page 91
- *Changing the Bootloader Timeout* on Page 92
- *Determining the Bootloader Version* on Page 92
- *Resetting the ICDM-RX/TCP-16RJ45/2RJ45-PM* on Page 93
- *Configuring Passwords* on Page 93
- *RedBoot Command Overview* on Page 94

Optionally, you can install PortVision DX on a Windows system on the network and perform all of these tasks. PortVision DX provides a Telnet/SSH session, which is discussed in *Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)* on Page 86.

9.1. Accessing RedBoot Overview

To access RedBoot, you can use one of the following methods:

- A *serial* connection between Port 1 on the ICDM-RX/TCP-16RJ45/2RJ45-PM and a COM port on a PC (Page 89). If you plan on using the serial method, you will need a null modem cable, a terminal program installed and configured on the PC, and a **Bootloader Timeout** value in excess of 15 seconds. If the **Bootloader Timeout** value has been reduced to 1 second, this procedure will NOT be possible.

  Note: *Use the serial connection method, if the ICDM-RX/TCP-16RJ45/2RJ45-PM is not on the same Ethernet network segment as the PC.*

  If you do not know the IP address of the ICDM-RX/TCP-16RJ45/2RJ45-PM you must use a serial connection to communicate with the ICDM-RX/TCP-16RJ45/2RJ45-PM.

- A *telnet* connection (Page 90), if the ICDM-RX/TCP-16RJ45/2RJ45-PM is locally accessible by Ethernet. A *telnet connection* requires that you know the IP address. In addition, the IP address must also be valid for the network to which it is attached.

  For example: The network segment must be 192.168.250.x to telnet to the ICDM-RX/TCP-16RJ45/2RJ45-PM default IP address if you have not changed the IP address to operate on your network.

9.2. Establishing a Serial Connection

Use the following procedure to set up a serial connection with a terminal server program. You can use PuTTY (Windows) or Minicom (Linux) or optionally, PuTTY can be accessed from PortVision DX using **Tools > Applications > PuTTY**.

1. Connect a null-modem cable from an available COM port on your PC to **Port 1** on the ICDM-RX/TCP-16RJ45/2RJ45-PM.

   Note: *See Connecting Serial Devices on Page 76, if you need to build a null-modem cable.*

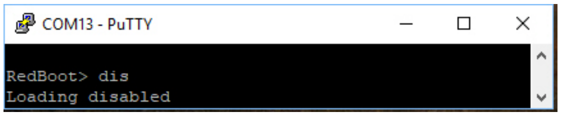
2. Configure the terminal server program to the following values:
   - Bits per second = 57600
   - Data bits = 8
   - Parity = None
   - Stop bits = 1
   - Flow control = None

   Note: *If you do not disable Bootloader from loading (Steps 3 through 5) within the time-out period (default is fifteen seconds), an application will be loaded from flash and started. If this happens, repeat Steps 3 through 5. The* ***#!DM*** *command is the only case-sensitive command and must be in uppercase.*

3. Reset the ICDM-RX/TCP-16RJ45/2RJ45-PM.

   Note: *Depending on the model, disconnect and reconnect the power cable (external power supply and no power switch) or turn the power switch on and then off (internal power supply).*

4. Immediately type **#!DM** and press **Enter** in the terminal program.



```
RedBoot> dis
Loading disabled
```

5. At the **RedBoot>** prompt, type **dis**, and press **Enter**.
6. Verify that loading has been disabled.
7. You can use the appropriate procedure listed on Page 88 or use the *RedBoot Command Overview* on Page 94 to perform the desired task.

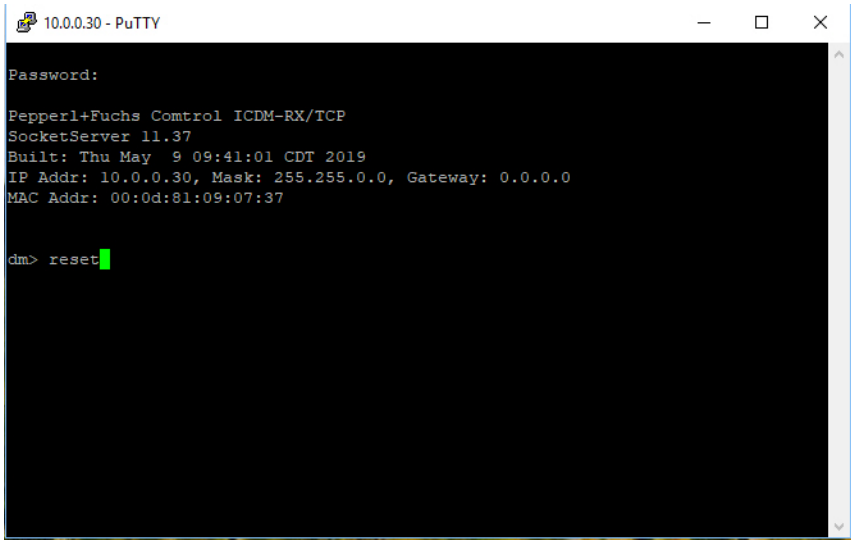
9.3. Establishing a Telnet Connection

Use the following procedure to telnet to the ICDM-RX/TCP-16RJ45/2RJ45-PM.

1. Open a telnet session, enter the ICDM-RX/TCP-16RJ45/2RJ45-PM IP address.

   If using Windows, you can use PortVision DX, see *Accessing RedBoot Commands in Telnet/SSH Sessions (PortVision DX)* on Page 86.

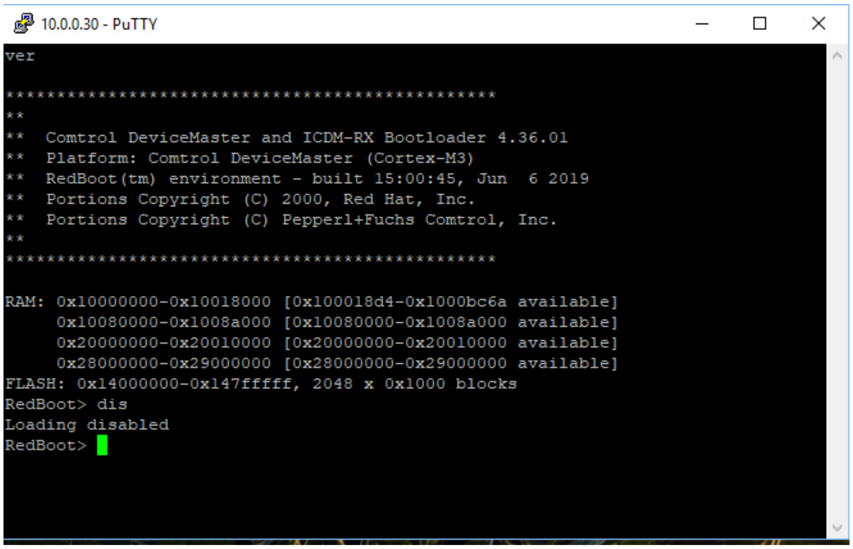
2. Press the **Enter** key if you did not program a password or type the password and press **Enter**.



```
Password:

Pepperl+Fuchs Comtrol ICDM-RX/TCP
SocketServer 11.37
Built: Thu May  9 09:41:01 CDT 2019
IP Addr: 10.0.0.30, Mask: 255.255.0.0, Gateway: 0.0.0.0
MAC Addr: 00:0d:81:09:07:37


dm> reset
```

Note: *The ICDM-RX/TCP-16RJ45/2RJ45-PM does not come pre-programmed with a password.*

3. Type **reset**, and close the session.
4. Open a new telnet session, enter the ICDM-RX/TCP-16RJ45/2RJ45-PM IP address, and the password.
5. Type **dis** to disable the Bootloader.
6. Verify that the system responds with a **Loading disabled** message.



```
ver

************************************************
**
**   Comtrol DeviceMaster and ICDM-RX Bootloader 4.36.01
**   Platform: Comtrol DeviceMaster (Cortex-M3)
**   RedBoot(tm) environment - built 15:00:45, Jun  6 2019
**   Portions Copyright (C) 2000, Red Hat, Inc.
**   Portions Copyright (C) Pepperl+Fuchs Comtrol, Inc.
**
************************************************

RAM: 0x10000000-0x10018000 [0x100018d4-0x1000bc6a available]
     0x10080000-0x1008a000 [0x10080000-0x1008a000 available]
     0x20000000-0x20010000 [0x20000000-0x20010000 available]
     0x28000000-0x29000000 [0x28000000-0x29000000 available]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks
RedBoot> dis
Loading disabled
RedBoot>
```

9.4. Determining the Network Settings

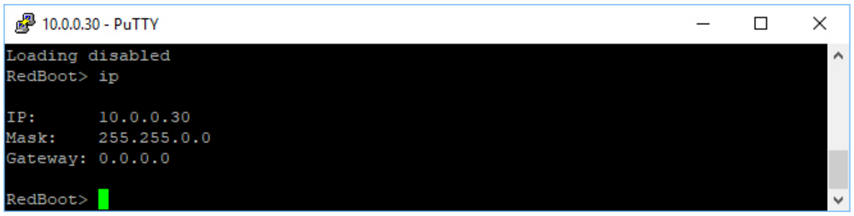
If you are not sure what the network information is on an ICDM-RX/TCP-16RJ45/2RJ45-PM, you can perform the following procedure.

The default network settings are:

- IP address: 192.168.250.250
- Subnet mask: 255.255.0.0
- Gateway address: 192.168.250.1

1. Establish communications with the ICDM-RX/TCP-16RJ45/2RJ45-PM using the serial (Page 89) or telnet (Page 90) method.
2. At the **RedBoot** prompt, type **ip**.

The IP address, subnet mask, and IP gateway values will display.



```
Loading disabled
RedBoot> ip

IP:      10.0.0.30
Mask:    255.255.0.0
Gateway: 0.0.0.0

RedBoot>
```

Note: *Optionally, you can install PortVision DX on a Windows system on the network and see the IP information.*

9.5. Configuring the Network Settings

Use the following procedure to program the IP address using RedBoot.

1. Establish communications with the ICDM-RX/TCP-16RJ45/2RJ45-PM using the serial (Page 89) or telnet (Page 90) method.
2. Enter **ip [*addr mask gateway*]** and press the **Enter** key to configure the IP address. *Where*:

   addr = IP address you want to use

   mask = matches you network subnet mask

   gateway = assigned by your network administrator

   Make sure that each value is separated by a space.

```
RedBoot>dis
Loading disabled
RedBoot> ip 192.168.11.152 255.255.0.0 192.168.0.254
RedBoot>
IP:     192.168.11.152
Mask:   255.255.00
Gateway: 192.168.0.254
RedBoot> reset
.. Resetting
```

3. Verify that RedBoot responds with your configured network information or reissue the command.
4. Type **reset** to reset the ICDM-RX/TCP-16RJ45/2RJ45-PM, if you do not have any other related RedBoot tasks.

9.6. Changing the Bootloader Timeout

Use the following procedure to change the Bootloader timeout value.

1. Establish communications with the ICDM-RX/TCP-16RJ45/2RJ45-PM using the serial (Page 89) or telnet (Page 90) method.
2. At the **RedBoot** prompt, type **timeout.**

```
RedBoot> dis
Loading disabled
RedBoot> timeout
Timeout 15 seconds
RedBoot> timeout 45
timeout 45 seconds
RedBoot>_
```

   RedBoot responds with the current Bootloader timeout value.

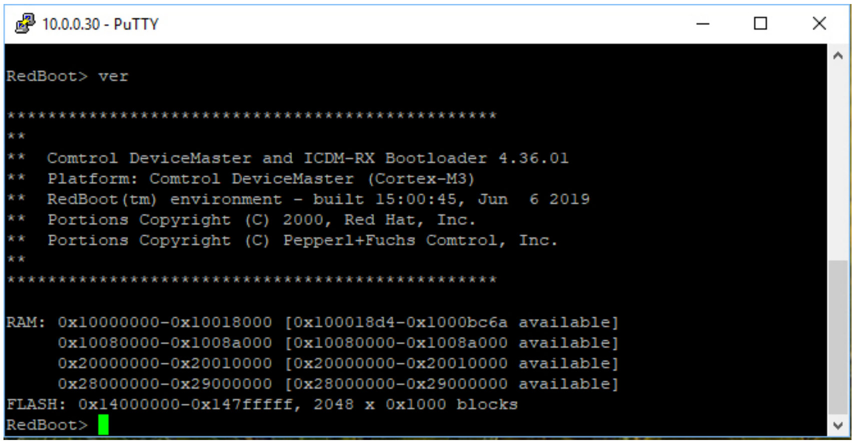
3. Type **timeout** and a value to change the timeout value. For example, **timeout 45** to change the Bootloader timeout to 45 seconds.

9.7. Determining the Bootloader Version

Use the following procedure to determine what Bootloader version is loaded in the ICDM-RX/TCP-16RJ45/2RJ45-PM.

1. Establish communications with the ICDM-RX/TCP-16RJ45/2RJ45-PM using the serial (Page 89) or telnet (Page 90) method.
2. At the **RedBoot** prompt, type **version**.

   The Bootloader information displays.



```
RedBoot> ver

************************************************
**
**   Comtrol DeviceMaster and ICDM-RX Bootloader 4.36.01
**   Platform: Comtrol DeviceMaster (Cortex-M3)
**   RedBoot(tm) environment - built 15:00:45, Jun  6 2019
**   Portions Copyright (C) 2000, Red Hat, Inc.
**   Portions Copyright (C) Pepperl+Fuchs Comtrol, Inc.
**
************************************************

RAM: 0x10000000-0x10018000 [0x100018d4-0x1000bc6a available]
     0x10080000-0x1008a000 [0x10080000-0x1008a000 available]
     0x20000000-0x20010000 [0x20000000-0x20010000 available]
     0x28000000-0x29000000 [0x28000000-0x29000000 available]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks
RedBoot>
```

3. Type **reset** to reset the ICDM-RX/TCP-16RJ45/2RJ45-PM, if you do not have any other related RedBoot tasks.

Note: *Optionally, you can install PortVision DX on a Windows system on the network and see the Bootloader version. Reboot the ICDM-RX/TCP-16RJ45/2RJ45-PM, right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM and click Refresh Device until the Bootloader version displays. The Bootloader version is only displayed for a few moments.*

9.8. Resetting the ICDM-RX/TCP-16RJ45/2RJ45-PM

When you have completed your tasks in RedBoot, you must enter a **reset** command at the **RedBoot**> prompt for the ICDM-RX/TCP-16RJ45/2RJ45-PM to begin operation.

Note: *The LEDs on the ICDM-RX/TCP-16RJ45/2RJ45-PM will go through the power up sequence. The ICDM-RX/TCP-16RJ45/2RJ45-PM has completed its reset cycle when the* ***PWR*** *or* ***Status*** *LED is lit and it stops flashing.*

```
RedBoot> dis
Loading disabled
RedBoot> reset
```

9.9. Configuring Passwords

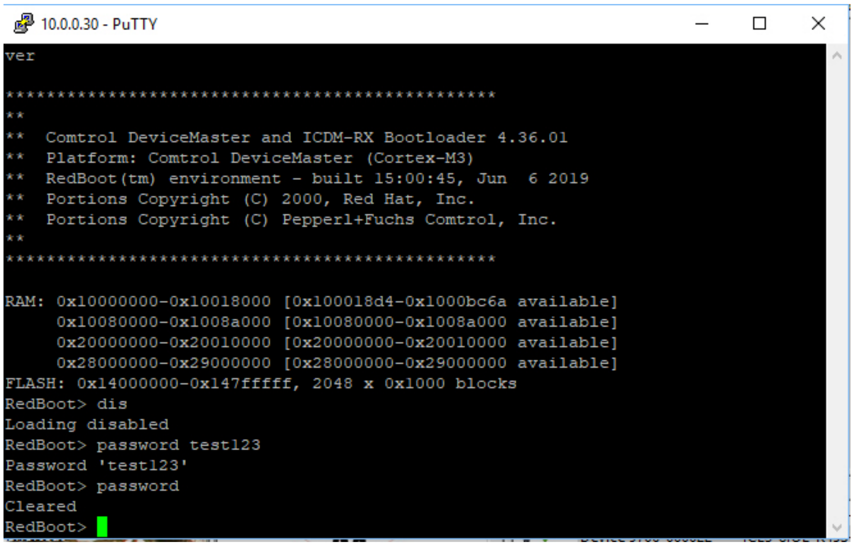
This section discusses how to configure a password for the web and telnet server.

Note: *See the PortVision DX or SocketServer Help system for information about email notification.*

Use the following procedure to establish the ICDM-RX/TCP-16RJ45/2RJ45-PM password for the Web and telnet server. Establishing a password prevents unauthorized changes to the ICDM-RX/TCP-16RJ45/2RJ45-PM configuration.

1. Establish communications with the ICDM-RX/TCP-16RJ45/2RJ45-PM using the serial (Page 89) or telnet method (Page 90).
2. Type **password** [**your_password**] and press **Enter**.

   Note: *If you forget your password, you can reprogram the password using the serial method which bypasses the password.*



```
ver

************************************************
**
**  Comtrol DeviceMaster and ICDM-RX Bootloader 4.36.01
**  Platform: Comtrol DeviceMaster (Cortex-M3)
**  RedBoot(tm) environment - built 15:00:45, Jun  6 2019
**  Portions Copyright (C) 2000, Red Hat, Inc.
**  Portions Copyright (C) Pepperl+Fuchs Comtrol, Inc.
**
************************************************

RAM: 0x10000000-0x10018000 [0x100018d4-0x1000bc6a available]
     0x10080000-0x1008a000 [0x10080000-0x1008a000 available]
     0x20000000-0x20010000 [0x20000000-0x20010000 available]
     0x28000000-0x29000000 [0x28000000-0x29000000 available]
FLASH: 0x14000000-0x147fffff, 2048 x 0x1000 blocks
RedBoot> dis
Loading disabled
RedBoot> password test123
Password 'test123'
RedBoot> password
Cleared
RedBoot>
```

Note: *The Bootloader version on your ICDM-RX/TCP-16RJ45/2RJ45-PM may be different than the version displayed in this above.*

See the **auth** command in the *RedBoot Command Overview* on Page 94, if you want to set up Web browser authentication.

9.10. RedBoot Command Overview

The following table is an overview of RedBoot commands available. After accessing RedBoot, you can review the list of commands on-line by entering **help** and pressing the **Enter** key..

<table>
<tr><th colspan="2">RedBoot Commands</th></tr>
<tr><td><b>auth</b>
<b>{noaccess, none, basic, md5, invalid}</b></td><td>Sets or displays web authentication. The default is set to <b>none</b>, which means that there is no authentication required to access the web server.
To deny access to the web server, click <b>noaccess</b> or <b>invalid</b>. If access is attempted, a message appears to notify the user that access is denied.
To configure the web server to request an un-encrypted password, click <b>basic</b>. To configure the web server to request an encrypted password, click <b>md5</b>. (Some browsers do not support the <b>md5</b> command.)</td></tr>
<tr><td><b>baudrate [-b <rate>]</b></td><td>Set/Query the system console baud rate.</td></tr>
<tr><td><b>boardrev†</b></td><td>Displays the board revision.</td></tr>
<tr><td><b>cache [ON | OFF]</b></td><td>Manages machine caches.</td></tr>
<tr><td><b>catalognum [catalog number]†</b></td><td>Shows catalog number.</td></tr>
<tr><td><b>channel [-1|<channel number>]</b></td><td>Displays or switches the console channel.</td></tr>
<tr><td><b>chassis†</b></td><td>Displays chassis information.</td></tr>
<tr><td><b>cksum -b <location> -l <length></b></td><td>Computes a 32-bit checksum [POSIX algorithm] for a range of memory.</td></tr>
<tr><td><b>clearconfig</b></td><td>Clears the application configuration.</td></tr>
<tr><td><b>cpufreq†</b></td><td>Shows CPU clock frequency.</td></tr>
<tr><td><b>delaycal <passes>†</b></td><td>Calibrates SDRAM clock delay.</td></tr>
<tr><td><b>deviceid [device id]†</b></td><td>Shows the Device ID.</td></tr>
<tr><td><b>disable</b></td><td>Disables automatic load of the default application.</td></tr>
<tr><td><b>dump -b <location> [-l <length>] [-s] [-1|-2|-4]</b></td><td>Display (hex dump) a range of memory.</td></tr>
<tr><td><b>eepromvers [ver]†</b></td><td>Shows the eeprom version.</td></tr>
<tr><td><b>fis {cmds}</b></td><td>Manages flash images.</td></tr>
<tr><td><b>flash</b></td><td>Shows flash information.</td></tr>
<tr><td><b>go [-w <timeout>] [-c] [-n] [entry]</b></td><td>Executes code at a location.</td></tr>
<tr><td><b>help <topic></b></td><td>Displays available RedBoot commands.</td></tr>
<tr><td><b>history</b></td><td>Displays command history.</td></tr>
<tr><td><b>hwflags†</b></td><td>Shows the HW feature flags.</td></tr>
<tr><td><b>ip [addr mask gateway]</b></td><td>Displays or sets the IP address configuration.</td></tr>
<tr><td><b>load [-r] [-v] [-h <host>]</b>
<b>[-p <TCP port>]</b>
<b>[-m <varies>]</b>
<b>[-c <channel_number>]</b>
<b>[-b <base_address>]</b>
<b><file_name></b></td><td>Loads a file.</td></tr>
<tr><td><b>loop 232|422|int port-number</b></td><td>Runs a loopback test on the port.</td></tr>
<tr><td><b>mac†</b></td><td>Displays the Ethernet MAC address.</td></tr>
</table>

RedBoot Commands (Continued)	
mcmp -s <location> -d <location> -l <length> [-1|-2|-4]	Compares two blocks of memory.
mcopy -s <location> -d <location> -l <length> [-1|-2|-4]	Copies memory from one address to another.
mem_read <start_addr> (<end_addr>)	Reads from memory.
mem_write <value> <start_addr> (<end_addr>)	Writes to memory.
mfill -b <location> -l <length> -p <pattern> [-1|-2|-4]	Fills a block of memory with a pattern.
model [model-number]†	Shows the model number.
modelname [model name]†	Shows the model name.
numether [num]†	Shows the number of Ethernet ports.
numserial [num]†	Shows the number of serial ports.
oemid [id]†	Shows the OEM ID.
password {password}	Sets or deletes the password.
ping [-v] [-n <count>] [-l <length>] [-t <timeout>] [-r <rate>] [-i <IP_addr>] -h <IP_addr>	Network connectivity test.
ramtest <passes>	Tests the RAM.
ramtime [reg [<value>]]	Shows RAM timing register values.
reset	Resets the ICDM-RX/TCP-16RJ45/2RJ45-PM.
secureconf [disable|enable]	Sets or displays secure config enable.
securedata [disable|enable]	Sets or displays secure data enable.
sernum [prefix] [serial_number] sernum [serial_number]†	Displays device serial number (if available).
?	Displays short help.
snmp [disable|enable]	Sets or displays SNMP enable.
summary	Displays a summary that includes the bootloader version, network address information, MAC address, and security settings.
telnet [disable | enable}	Sets or displays telnet server enable. Disables telnet.
teltimeout [seconds]	Shows or sets telnet time-out.
terse	Terse command response mode.
t485 port #1 port #2	Runs port-to-port RS-485 test. Port numbering is Port 0 through 15 and you must connect a straight-through cable such as Ethernet patch cord.
timeout {seconds}	Displays or sets Bootloader time-out value.
vendorid [vendor id]†	Shows the vendor ID.
version	Displays RedBoot version information.
x -b <location> [-l <length>] [-s] [-1|-2|-4]	Display (hex dump) a range of memory.
kszdump	Dump pre-determined set of KSZ8863 registers.

RedBoot Commands (Continued)	
kszrd <r1> [r2]	Read specified KSZ8863 registers.
kszrestart	Restart KSZ8863.
kszwr <r1> <val>	Read specified KSZ8863 registers.
† *Read-only items that you cannot change in Redboot.*	

10. External Power Supply Specifications

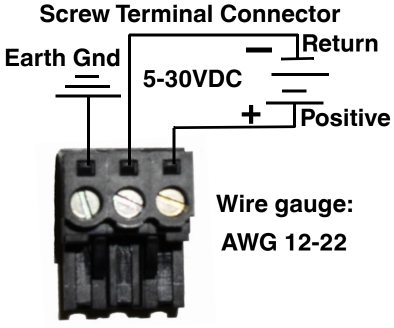
This section discusses information that you may need if you wish to use your own external power supplies.

10.1. ICDM-RX/TCP-16RJ45/2RJ45-PM Power Supply

This table provides specifications for the optional power supply from Pepperl+Fuchs.

Pepperl+Fuchs Power Supply: ICDM-RX/TCP-DB9/RJ45-PM	
Input line frequency Input line voltage Output voltage Output current	43-63 Hz 90-260 VAC 24VDC 275 mA @ 24VDC

This table provides the specifications, if you intend on using your own power supply.



ICDM-RX/TCP-DB9/RJ45-PM External Power Supply	
Output voltage† Current† Power	5-30VDC 200 mA (Min) @ 24VDC 4.5 W
† *Any power supply that meets current consumption, voltage, power, and connector pin outs requirements can be used.*	

4/27/22

11. Troubleshooting and Technical Support

This section contains troubleshooting information for your ICDM-RX/TCP-16RJ45/2RJ45-PM. You may want to review the following subsections before calling Technical Support because they will request that you perform many of the procedures or verifications before they will be able to help you diagnose a problem.

- *Troubleshooting Checklist* on Page 99
- *General Troubleshooting* on Page 100
- *Testing Ports Using Port Monitor (PMon2)* on Page 102
- *Testing Ports Using Test Terminal* on Page 106
- *Socket Mode Serial Port Testing* on Page 113
- *Daisy-Chaining ICDM-RX/TCP-16RJ45/2RJ45-PM With Dual Ethernet Ports* on Page 119
- *ICDM-RX/TCP-16RJ45/2RJ45-PM LEDs* on Page 120
- *Removing ICDM-RX/TCP-16RJ45/2RJ45-PM Security Features* on Page 121

If you cannot diagnose the problem, you can contact Technical Support.

11.1. Troubleshooting Checklist

The following checklist may help you diagnose your problem:

- Verify that you are using the correct types of cables on the correct connectors and that all cables are connected securely.

  Note: *Most customer problems reported to Pepperl+Fuchs Technical Support are eventually traced to cabling or network problems.*

- Verify that the network IP address, subnet mask, and gateway is correct and appropriate for the network. Make sure that the IP address programmed into the ICDM-RX/TCP-16RJ45/2RJ45-PM matches the unique reserved IP configured address assigned by the system administrator.
  - If IP addressing is being used, the system should be able to ping the ICDM-RX/TCP-16RJ45/2RJ45-PM.
  - If using DHCP, the host system needs to provide the subnet mask and gateway.
- Verify that the Ethernet hub and any other network devices between the system and the ICDM-RX/TCP-16RJ45/2RJ45-PM are powered up and operating.
- Verify that the hardware MAC address in the NS-Link device driver matches the address on the ICDM-RX/TCP-16RJ45/2RJ45-PM.
- If using a driver for Windows, verify that you are addressing the port correctly. In many applications, device names above COM9 require the prefix **\\.** in order to be recognized. For example, to reference COM20, use **\\.\COM20** as the file or port name.
- If using a driver for Windows, you can use one of the Pepperl+Fuchs tools.
  - *Advanced* tab in the *Windows Drivers Management Console* which helps identify problems.
  - PortVision DX contains two applications that can be used to test or monitor the ICDM-RX/TCP-16RJ45/2RJ45-PM:
    - *Test Terminal* program, which can be used to troubleshoot communications on a port-by-port basis. See *Testing Ports Using Test Terminal* on Page 106 for testing procedures.
    - *Port Monitor* program, which checks for errors, modem control, and status signals. In addition, it provides you with raw byte input and output counts. See *Testing Ports Using Port Monitor (PMon2)*

on Page 102 for procedures.

- Enable the **Verbose Event Log** feature on the **Device General** tab and then reboot the system.

- Reboot the system, then reset the power on the ICDM-RX/TCP-16RJ45/2RJ45-PM and watch the **PWR** or **Status** (Page 120) light activity.

PWR or Status LED	Description
5 sec. off, 3 flashes, 5 sec. off, 3 flashes...	RedBoot^{TM} checksum failure.
5 sec. off, 4 flashes, 5 sec. off, 4 flashes...	SREC load failure.

Note: *If the device has a power switch, turn the device's power switch off and on, while watching the LED diagnostics. If the ICDM-RX/TCP-16RJ45/2RJ45-PM does not have a power switch, disconnect and reconnect the power cord.*

- Remove and reinstall the ICDM-RX/TCP-16RJ45/2RJ45-PM NS-Link device driver.
- If you have a spare ICDM-RX/TCP-16RJ45/2RJ45-PM, try replacing the device.

11.2. General Troubleshooting

This table illustrates some general troubleshooting tips.

Note: *Make sure that you have reviewed the Troubleshooting Checklist on Page 99.*

General Condition	Explanation/Action
PWR or **Status** LED flashing	Indicates that the bootloader has not downloaded to the ICDM-RX/TCP-16RJ45/2RJ45-PM. 1. If applicable, remove the NS-Link driver. 2. Make sure that you have downloaded the most current driver from https://www.pepperl-fuchs.com. 3. Install the latest driver and configure the ICDM-RX/TCP-16RJ45/2RJ45-PM using the MAC address. Make sure that you reboot the system. See *Device Driver (NS-Link) Installation* on Page 17 for procedures. ***Note:*** *If the **PWR** or **Status** LED is still flashing, contact Technical Support.*
Can ping the Pepperl+Fuchs device, but cannot open the ports from a remote location. (You must have previously programmed the IP address, subnet mask, and IP gateway.)	The NS-Link driver uses Port 4606 (**11FE** h) to communicate with the ICDM-RX. When using a *sniffer* to track NS-Link packets, filtering for Port 4606 will easily track the packet. The packet should also contain the MAC address of the device and the originating PC so that it can be determined if the packet is able to travel the full distance one way or not. If the 4606 packet is found on one side of a firewall or router, using sniffer, and not on the other side, then that port needs to be opened up to allow the 4606 to pass. This will most often be seen with firewalls, but is also seen in some routers.
Cannot ping the device through Ethernet hub	Isolate the ICDM-RX/TCP-16RJ45/2RJ45-PM from the network. Connect the device directly to the NIC in the host system.

General Condition	Explanation/Action
Cannot ping or connect to the ICDM-RX/TCP-16RJ45/2RJ45-PM	The default ICDM-RX/TCP-16RJ45/2RJ45-PM IP address is often not accessible due to the subnet masking from another network unless **192.168** is used in the network. In most cases, it will be necessary to program in an address that conforms to your network. See *Configuring the Network Settings (PortVision DX)* on Page 14 to use PortVision DX to program the IP address. If you do not use PortVision DX (or the NS-Link driver for Windows) to program the IP address, you can use RedBoot. If you use RedBoot, you only have 15 seconds to disable the Bootloader with RedBoot to get into the setup utility. See *RedBoot Procedures* on Page 88 for the RedBoot method of programming an IP address.
ICDM-RX/TCP-16RJ45/2RJ45-PM continuously reboots when connected to some Ethernet switches with the NS-Link driver	The problem is caused by a L2 bridging feature called Spanning Tree Algorithm (STA) in the switch. This feature is enabled by default in some switches. This features causes time-out problems on certain L2 protocols, such as our MAC mode. *Resolution*: There will be no firmware fix for this problem. Only ***one*** of the following fixes is required for resolution. 1. Disable STA in the switch. 2. Enable STA fast forwarding on the port. 3. Change the STA Forward Delay and Message Age to minimum time values. 4. On the device, set the time-out value to 0 (to disable loading of SocketServer) or 120. The command from the redboot prompt is “Timeout 120” without the quotes. *Problem Details*: STA by default blocks packets for 30 seconds after an Ethernet port auto negotiates. Blocking of these packets causes the NS-Link driver load process to fail. The normal NS-Link driver load process is: 1. If NS-Link determines that it needs to load a device, it resets the device. It does this to get the device into RedBoot mode. Only RedBoot accepts **load binary** commands, which are needed to load the NS-Link binary into the ICDM-RX/TCP-16RJ45/2RJ45-PM. 2. After a 6 second delay, NS-Link sends an ID query to the device. This query is to verify that the device is in RedBoot and can accept **load binary** commands. 3. The device sends an ID query response. 4. NS-Link loads the device. If the device is not loaded after **timeout** seconds (default 15), it loads SocketServer. The above process fails when STA is running because the switch blocks packets for 30 seconds after the ICDM-RX/TCP-16RJ45/2RJ45-PM reboots. Therefore, the ID query is not received by the ICDM-RX/TCP-16RJ45/2RJ45-PM and after 15 seconds the device loads SocketServer. After 30 seconds, NS-Link finally can do an ID query, which reveals that the device is not in RedBoot. NS-Link therefore reboots the device, and the process repeats.
ICDM-RX/TCP-16RJ45/2RJ45-PM continuously reboots when connected to some Ethernet switches or routers	Invalid IP information may also cause the switch or router to check for a gateway address. Lack of a gateway address is a common cause.

11.3. Testing Ports Using Port Monitor (PMon2)

You can use this subsection to test the ICDM-RX/TCP-16RJ45/2RJ45-PM driver installation. If you need to install the device driver, locate the latest driver from: https://www.pepperl-fuchs.com.

11.3.1.Overview

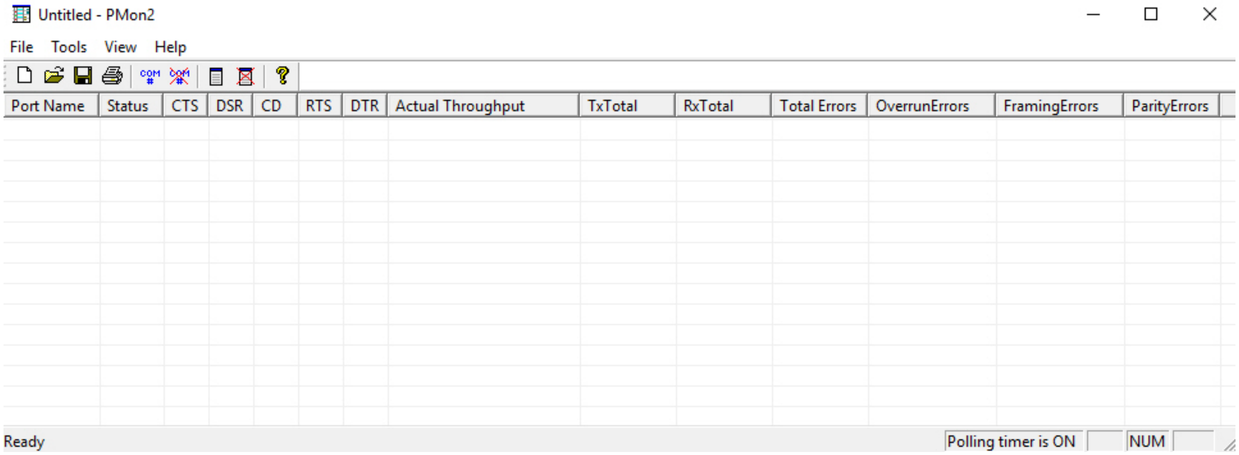
This procedure will check whether the ICDM-RX/TCP-16RJ45/2RJ45-PM can:

- Communicate through the Pepperl+Fuchs device driver
- Determine if a port is open with an application

11.3.2.Testing Pepperl+Fuchs COM Ports With Port Monitor

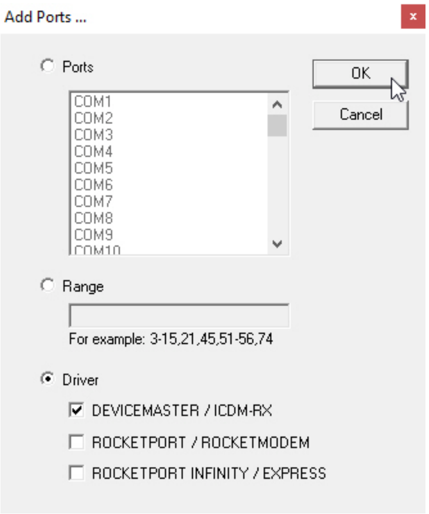
If necessary, *Installing PortVision DX* on Page 13 to install PortVision DX, which contains Port Monitor.

1. Start PortVision DX from the **Start** menu, select **Pepperl+Fuchs Comtrol** > **PortVision DX** or click the desktop shortcut.
2. Select **Tools** > **Applications** > **Port Monitor (PMon2)**.
3. Click **Add Ports** using the icon or **Tools** > **Add Ports**,



Port Name	Status	CTS	DSR	CD	RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	OverrunErrors	FramingErrors	ParityErrors

4. Click **Driver**, click **DEVICEMASTER / ICDM-RX.**



Add Ports ...

○ Ports

COM1
COM2
COM3
COM4
COM5
COM6
COM7
COM8
COM9
COM10

○ Range

For example: 3-15,21,45,51-56,74

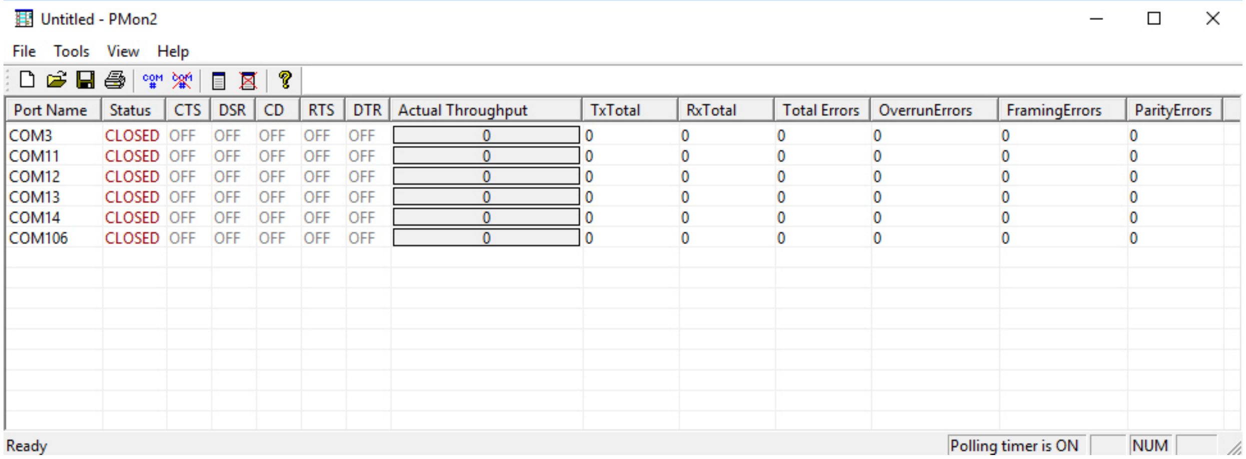
● Driver

☑ DEVICEMASTER / ICDM-RX

□ ROCKETPORT / ROCKETMODEM

□ ROCKETPORT INFINITY / EXPRESS

5. If the ICDM-RX/TCP-16RJ45/2RJ45-PM is communicating with the device driver for Windows, Port Monitor should display **CLOSED** status. If a port is open for an application, it displays as **OPEN**, and displays **Actual Throughput**, **TxTotal** and **RxTotal** statistics.



Untitled - PMon2

Port Name	Status	CTS	DSR	CD	RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	OverrunErrors	FramingErrors	ParityErrors
COM3	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM11	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM12	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM13	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM14	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0
COM106	CLOSED	OFF	OFF	OFF	OFF	OFF	0	0	0	0	0	0	0

Ready

Polling timer is ON

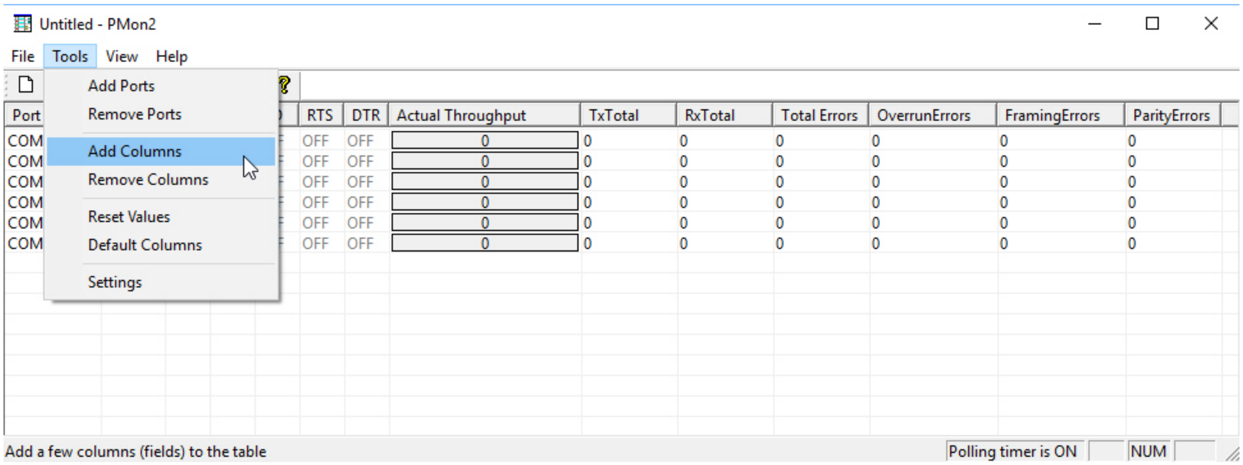
NUM

Normally, there should be no data errors recorded or they should be very small. To find out what the actual errors are, scroll to the right. You will see three columns: **Overrun Errors**, **Framing Errors**, and **Parity Errors**.

If the errors are:

- **Overrun Errors** represent receive buffer overflow errors. If this is the case, you will have to configure either software or hardware handshaking to control the flow of data. The most common errors are **Overrun** errors.
- **Framing Errors** indicate that there is an synchronization error between the beginning of a data frame and the end of the data frame. A frame usually consists of a start bit, 8 data bits, and a stop bit or two. The framing error occurs if the stop bit is not detected or it occurs in the wrong time frame. Most causes for framing errors are electrical noise on the data lines, or differences in the data clocks of the ICDM-RX/TCP-16RJ45/2RJ45-PM and the connected device.
- **Parity Errors** occur when parity is used and the parity bit is not what is expected. This can also be caused by noise on the data lines.

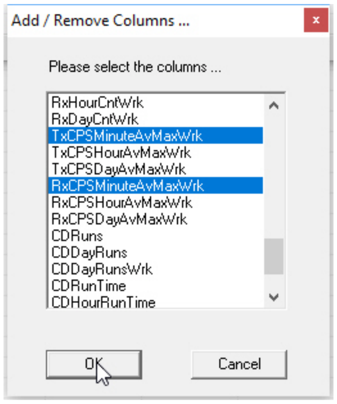
6. You can view additional statistics to Port Monitor by adding columns. Click **Tools** and **Add Columns**.



Port	RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	OverrunErrors	FramingErrors	ParityErrors
COM	OFF	OFF	0	0	0	0	0	0	0
COM	OFF	OFF	0	0	0	0	0	0	0
COM	OFF	OFF	0	0	0	0	0	0	0
COM	OFF	OFF	0	0	0	0	0	0	0
COM	OFF	OFF	0	0	0	0	0	0	0
COM	OFF	OFF	0	0	0	0	0	0	0

Add a few columns (fields) to the table

7. Highlight or shift-click to add multiple statistics and click **Ok**.

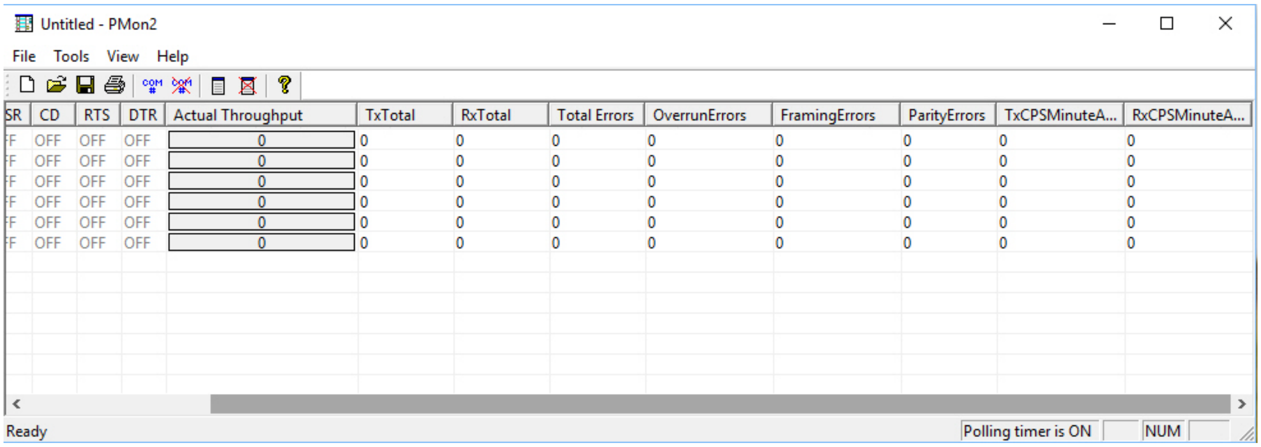


Please select the columns ...

- RxHourCntWrk
- RxDayCntWrk
- TxCPSMinuteAvMaxWrk
- TxCPSHourAvMaxWrk
- TxCPSDayAvMaxWrk
- RxCPSMinuteAvMaxWrk
- RxCPSHourAvMaxWrk
- RxCPSDayAvMaxWrk
- CDRuns
- CDDayRuns
- CDDayRunsWrk
- CDRunTime
- CDHourRunTime

Note: *See the Port Monitor help system if you need an explanation of a column.*

8. Scroll to the right to view the new columns.



SR	CD	RTS	DTR	Actual Throughput	TxTotal	RxTotal	Total Errors	OverrunErrors	FramingErrors	ParityErrors	TxCPSMinuteA...	RxCPSMinuteA...
F	OFF	OFF	OFF	0	0	0	0	0	0	0	0	0
F	OFF	OFF	OFF	0	0	0	0	0	0	0	0	0
F	OFF	OFF	OFF	0	0	0	0	0	0	0	0	0
F	OFF	OFF	OFF	0	0	0	0	0	0	0	0	0
F	OFF	OFF	OFF	0	0	0	0	0	0	0	0	0
F	OFF	OFF	OFF	0	0	0	0	0	0	0	0	0

Ready

9. If you want to capture this session, you can save a current session as a report. To do this, select one of the following save options:

   - **File > Save As**

- **File** > **Save** - if the report already exists in an older format
- **Save Active Session** button

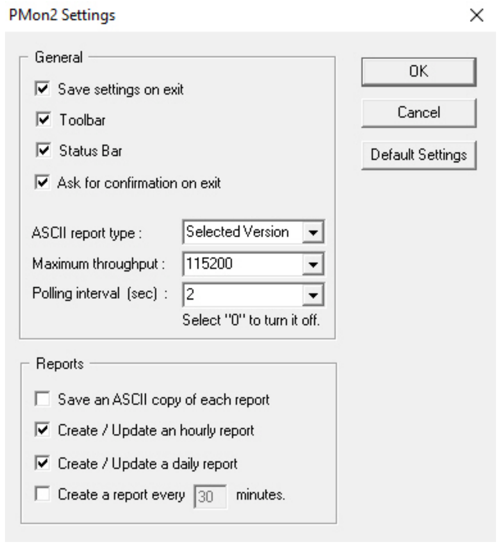
Reports can be opened, viewed and re-used when needed. To open and view a report:

a. **Select File** > **Open** or the **Open Existing Session** button. The *Open Session* dialog appears.

b. Locate the session (table), you want to open and click the **Open** button.

Optionally, if you want to continue monitoring for an existing session, you need to activate the *Polling Interval*.

- **Select Tools** > **Settings** to access the PMon2 *Settings* dialog
- Change the **Polling Interval** field to a value other than zero (0)



PMon2 Settings

General

☑ Save settings on exit

☑ Toolbar

☑ Status Bar

☑ Ask for confirmation on exit

ASCII report type : Selected Version

Maximum throughput : 115200

Polling interval (sec) : 2

Select "0" to turn it off.

Reports

☐ Save an ASCII copy of each report

☑ Create / Update an hourly report

☑ Create / Update a daily report

☐ Create a report every 30 minutes.

10. Leave Port Monitor open so that you can review events when using *Test Terminal* to test a port or ports.

11.4. Testing Ports Using Test Terminal

You can use the following procedure to test COM ports. If you need to install the ICDM-RX/TCP-16RJ45/2RJ45-PM device driver, locate the latest driver from: https://www.pepperl-fuchs.com.

The following procedures require a loopback plug to be placed on the port or ports that you want to test. A loopback plug was shipped with your product. If you need to build a replacement or additional loopback plugs, refer to *Connecting Serial Devices* on Page 62.

11.4.1.Overview

Test Terminal (WCom2) allows you to open a port, send characters and commands to the port, and toggle the control signals. This application can be used to troubleshoot communications on a port-by-port basis.

- **Send and Receive Test Data**: This sends data out the transmit line to the loopback plug, which has the transmit and receive pins connected thus sending the data back through the Rx line to Test Terminal, which then displays the received data in the terminal window for that port. This test is only testing the Tx and Rx signal lines and nothing else. This test works in either RS-232 or RS-422 modes as both modes have transmit and receive capability. A failure in this test will essentially prevent the port from working in any manner.
- **Loopback Test:** This tests all of the modem control signals such as RTS, DTR, CTS, DSR, CD, and RI along with the Tx and Rx signals. When a signal is made HI in one line the corresponding signal line indicates this. The Loopback Test changes the state of the lines and looks for the corresponding state change. If it successfully recognizes all of these changes, the port passes.

  A failure on this test is not necessarily critical as it will depend on what is connected and how many signal lines are in use. For example, if you are using RS-232 in 3-wire mode (Transmit, Receive and Ground) a failure will cause no discernible issue since the other signals are not being used. If the port is configured for use as either RS-422 or RS-485 this test will fail and is expected to fail since RS-422 and RS-485 do not have the modem control signals that are present in RS-232 for which this test is designed.

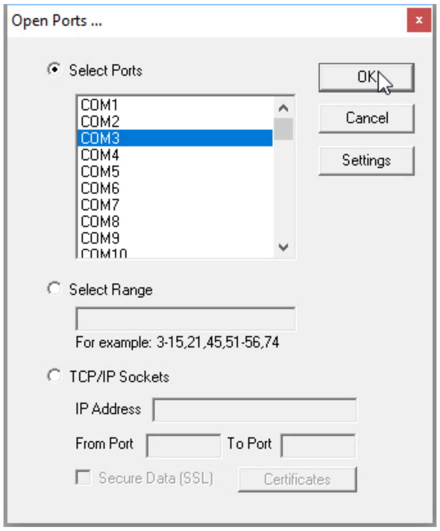
11.4.2.Opening Ports

The following procedure shows how to use **Test Terminal** to send and receive test data to the serial ports. If necessary, use *Installing PortVision DX* on Page 13, which contains Test Terminal.

1. Stop all applications that may be accessing the ports such as RRAS or any faxing, or production software. See the appropriate help systems or manuals for instructions on stopping these services or applications.

   If another application is controlling the port, then **Test Terminal** will be unable to open the port and an error message will be shown.
2. Start Test Terminal (WCom2). If necessary, start PortVision DX from the **Start** menu, select **Pepperl+Fuchs Comtrol > PortVision DX** or click the desktop shortcut.
3. Select **Tools** > **Applications** > **Test Terminal (WCom2)**.

4. Select **File** > **Open Port**, the appropriate port (or ports) from the *Open Ports* drop list and **Ok**.



Note: *If you left Port Monitor open from the previous subsection, you should show that the port is open.*

Go to the appropriate procedure to send and receive test data.

- *Sending and Receiving Test Data (RS-232/422/485: 4-Wire)* (below)
- *Sending and Receiving Data (RS-485: 2-Wire)* on Page 109

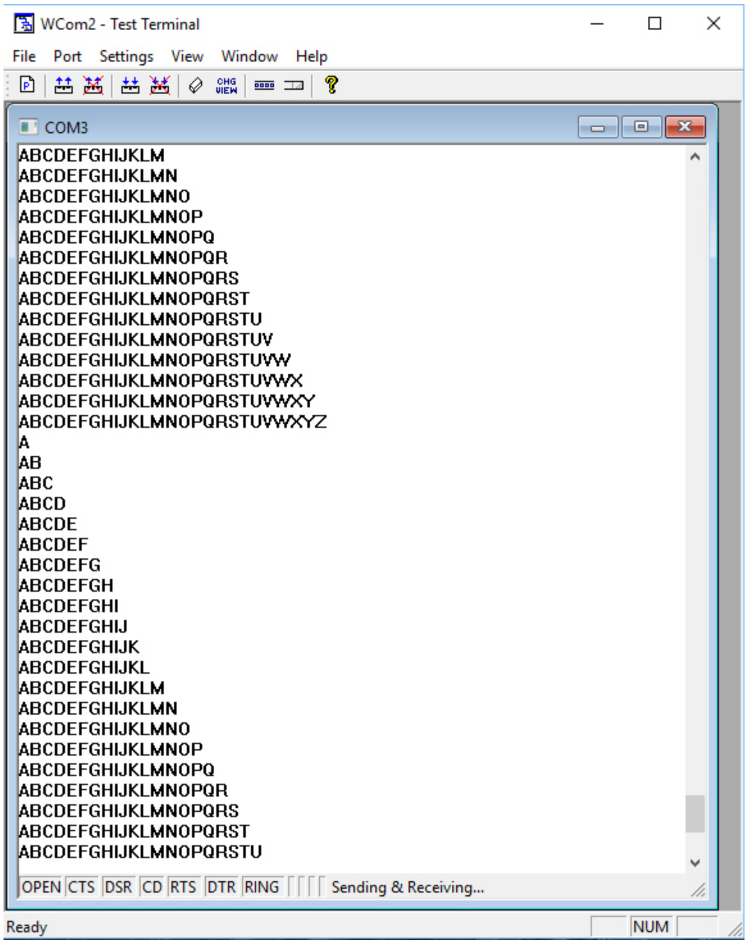
11.4.3.Sending and Receiving Test Data (RS-232/422/485: 4-Wire)

You can use this procedure to send and receive test data through the RS-232/422/485 (4-wire, full-duplex) port or ports that you want to test.

1. If you have not done so, perform Steps 1 through 2 on Page 106.
2. Install the loopback plug onto the port (or ports) that you want to test.

   See *Connecting Serial Devices* on Page 62, if you need to build loopback plugs.
3. Select **Port** > **Send and Receive Test Data**.

   You should see the alphabet scrolling across the port. If so, then the port installed properly and is operational.



```
ABCDEFGHIJKLM
ABCDEFGHIJKLMN
ABCDEFGHIJKLMNO
ABCDEFGHIJKLMNOP
ABCDEFGHIJKLMNOPQ
ABCDEFGHIJKLMNOPQR
ABCDEFGHIJKLMNOPQRS
ABCDEFGHIJKLMNOPQRST
ABCDEFGHIJKLMNOPQRSTU
ABCDEFGHIJKLMNOPQRSTUV
ABCDEFGHIJKLMNOPQRSTUVW
ABCDEFGHIJKLMNOPQRSTUVWX
ABCDEFGHIJKLMNOPQRSTUVWXY
ABCDEFGHIJKLMNOPQRSTUVWXYZ
A
AB
ABC
ABCD
ABCDE
ABCDEF
ABCDEFG
ABCDEFGH
ABCDEFGHI
ABCDEFGHIJ
ABCDEFGHIJK
ABCDEFGHIJKL
ABCDEFGHIJKLM
ABCDEFGHIJKLMN
ABCDEFGHIJKLMNO
ABCDEFGHIJKLMNOP
ABCDEFGHIJKLMNOPQ
ABCDEFGHIJKLMNOPQR
ABCDEFGHIJKLMNOPQRS
ABCDEFGHIJKLMNOPQRST
ABCDEFGHIJKLMNOPQRSTU
```

OPEN CTS DSR CD RTS DTR RING Sending & Receiving...

Ready NUM

Note: *If you left Port Monitor running, it should show data sent and received and show the average data throughput on the port.*

4. Select **Port** > **Send and Receive Test Data** to stop the scrolling data.
5. You can go to the next procedure to run the *Loopback Test* on Page 109 if this is an RS-232 port.

If this test successfully completed, then the port is operational as expected.

Note: *Do NOT forget to restart the communications application.*

11.4.4.Loopback Test (RS-232)

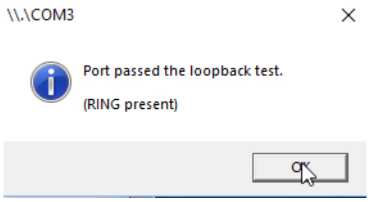
The **Loopback Test** tests the modem control (hardware handshaking) signals. It only has meaning in RS-232 mode on serial connector interfaces with full RS-232 signals. If performed under the following conditions, the test will always fail because full modem control signals are not present:

- RS-422
- RS-485

Use the following steps to run the Loopback Test.

1. If necessary, start Test Terminal (Page 106, Steps 1 through 2).
2. Click **Port > Loopback Test**.
3. If necessary, attach the loopback plug on the port or ports.
4. Click the **Ok** button after attaching the loopback plug.

   This is a pass fail test and will take a second or two to complete. Repeat for each port that needs testing.



\\.\COM3

Port passed the loopback test.

(RING present)

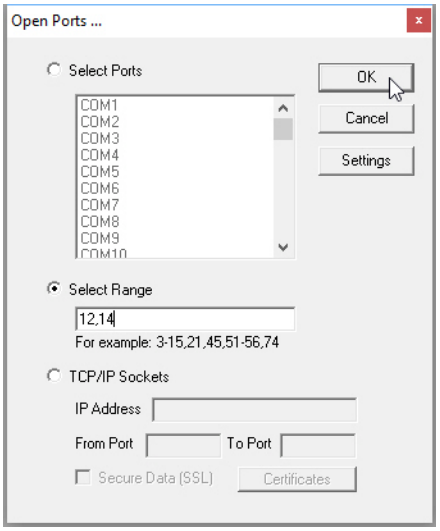
If the Loopback Test and the Send and Receive Test Data tests successfully complete, then the port is operational as expected.

11.4.5.Sending and Receiving Data (RS-485: 2-Wire)

This procedure shows how to use Test Terminal (WCom2) to test two RS-485 (2-Wire, Half-Duplex) ports.

Note: *See RJ45 Straight-Through Cables (RS-232/485) on Page 63 if you need to build a cable.*

1. In PortVision DX, click **Tools >Applications >Test Terminal (WCom2)** to start Test Terminal.
2. Open two ports RS-485 ports. This example uses COM12 and COM14.



Open Ports ...

○ Select Ports

COM1
COM2
COM3
COM4
COM5
COM6
COM7
COM8
COM9
COM10

● Select Range

12,14

For example: 3-15,21,45,51-56,74

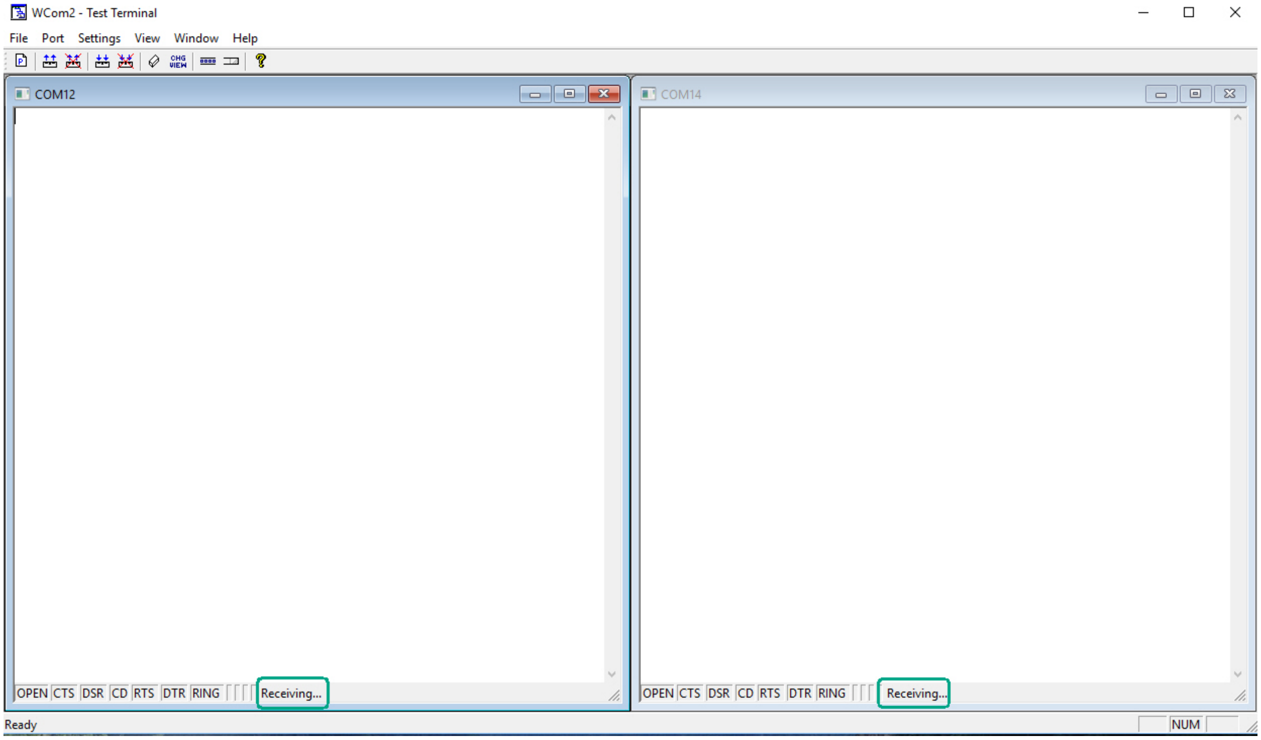
○ TCP/IP Sockets

IP Address

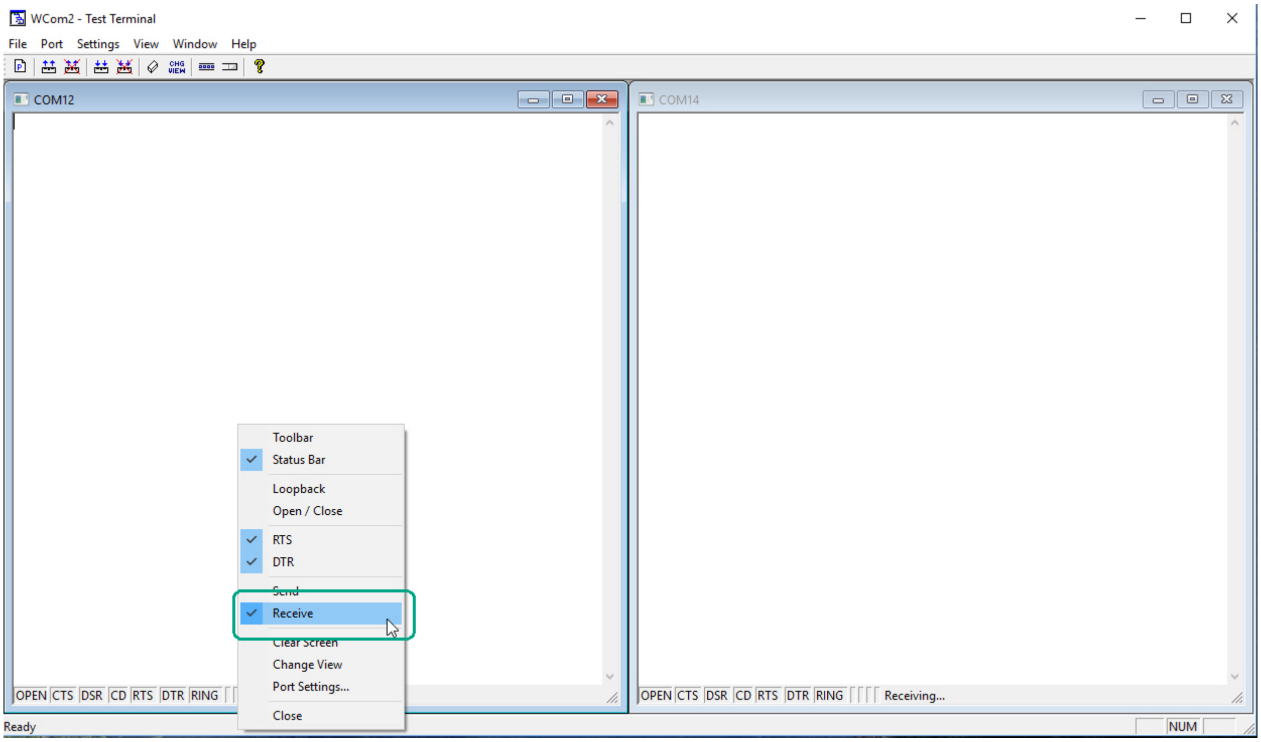
From Port To Port

□ Secure Data (SSL)

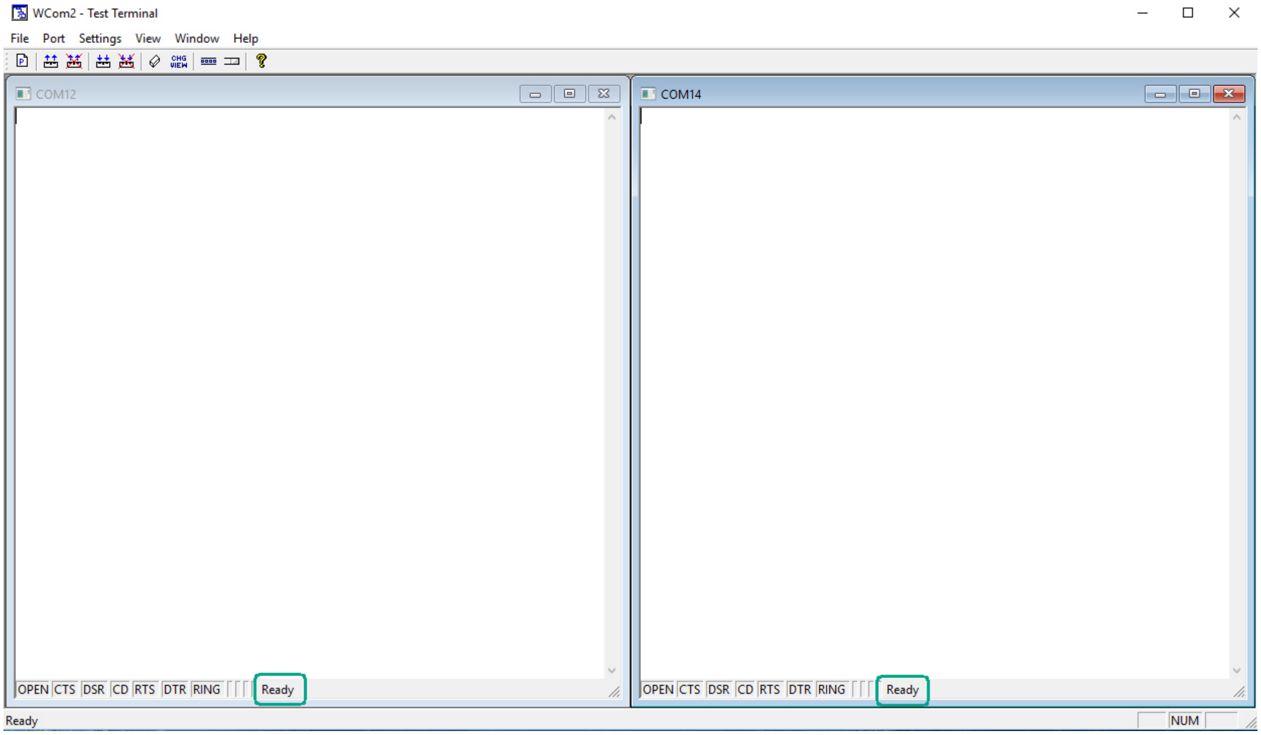
Test Terminal opens two windows, note that both ports show *Receiving* on the status bar.


WCom2 - Test Terminal
File Port Settings View Window Help
COM12
COM14
OPEN CTS DSR CD RTS DTR RING Receiving...
OPEN CTS DSR CD RTS DTR RING Receiving...
Ready
NUM

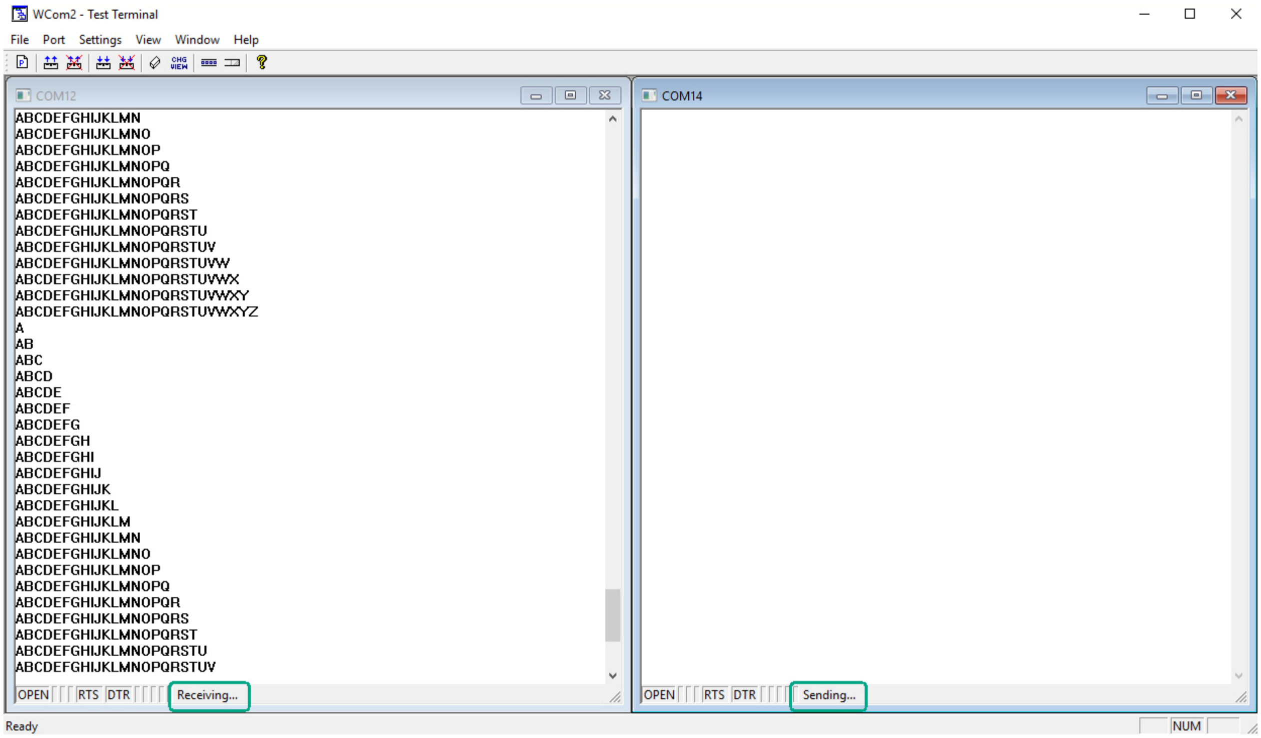
3. Right-click in both COM windows and remove the check mark for **Receive**.



Both COM ports show *Ready* on the status bar.



4. Right-click in ONE window and select the **Receive** option from the pop up.
5. Right-click the OPPOSITE window and click **Send**.



```
ABCDEFGHIJKLMN
ABCDEFGHIJKLMNO
ABCDEFGHIJKLMNOP
ABCDEFGHIJKLMNOPQ
ABCDEFGHIJKLMNOPQR
ABCDEFGHIJKLMNOPQRS
ABCDEFGHIJKLMNOPQRST
ABCDEFGHIJKLMNOPQRSTU
ABCDEFGHIJKLMNOPQRSTUV
ABCDEFGHIJKLMNOPQRSTUVW
ABCDEFGHIJKLMNOPQRSTUVWX
ABCDEFGHIJKLMNOPQRSTUVWXY
ABCDEFGHIJKLMNOPQRSTUVWXYZ
A
AB
ABC
ABCD
ABCDE
ABCDEF
ABCDEFG
ABCDEFGH
ABCDEFGHI
ABCDEFGHIJ
ABCDEFGHIJK
ABCDEFGHIJKL
ABCDEFGHIJKLM
ABCDEFGHIJKLMN
ABCDEFGHIJKLMNO
ABCDEFGHIJKLMNOP
ABCDEFGHIJKLMNOPQ
ABCDEFGHIJKLMNOPQR
ABCDEFGHIJKLMNOPQRS
ABCDEFGHIJKLMNOPQRST
ABCDEFGHIJKLMNOPQRSTU
ABCDEFGHIJKLMNOPQRSTUV
```

The *Status* line shows *Sending* or *Receiving*. In this case, COM14 is sending data and COM12 is receiving the data which is visually confirmed by the data scrolling across the COM12 window.

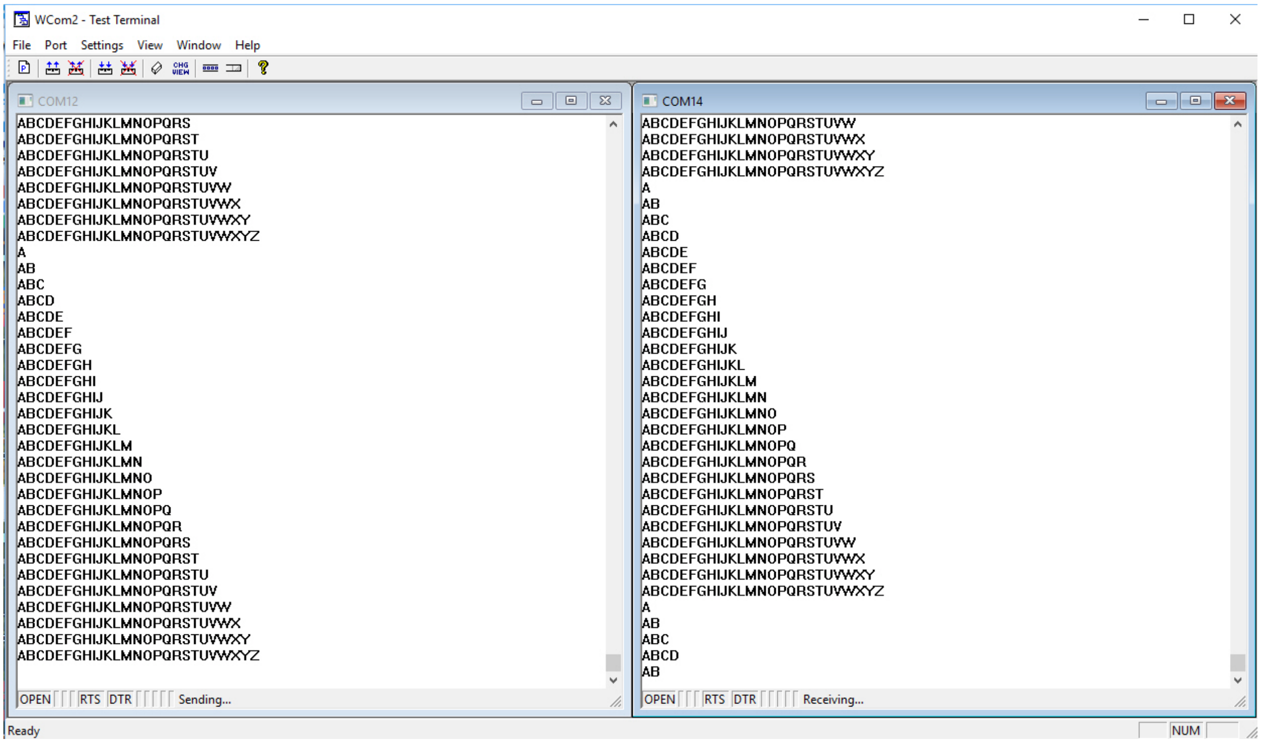
Note: *If you do not see the data being received it MAY be necessary to also disable the RTS and DTR options from the right-click pop-up menu in each COM port.*

6. Right-click and remove the check mark on the *Sending* COM port.
7. Right-click and remove the check mark on the *Receiving* COM port.

   Neither COM port is sending or receiving data but shows *Ready* on the *Status* bar.
8. Reverse the sending/receiving windows one at a time. Set the **Receive** option first, then in the opposite window, select the **Send** option.

   The *Status* line shows *Sending* or *Receiving* in the reverse windows.

Data is now scrolling in the COM14 window. COM12 is static as it is not receiving data but transmitting data.



COM12:

```
ABCDEFGHIJKLMNOPQRS
ABCDEFGHIJKLMNOPQRST
ABCDEFGHIJKLMNOPQRSTU
ABCDEFGHIJKLMNOPQRSTUV
ABCDEFGHIJKLMNOPQRSTUVW
ABCDEFGHIJKLMNOPQRSTUVWX
ABCDEFGHIJKLMNOPQRSTUVWXY
ABCDEFGHIJKLMNOPQRSTUVWXYZ
A
AB
ABC
ABCD
ABCDE
ABCDEF
ABCDEFG
ABCDEFGH
ABCDEFGHI
ABCDEFGHIJ
ABCDEFGHIJK
ABCDEFGHIJKL
ABCDEFGHIJKLM
ABCDEFGHIJKLMN
ABCDEFGHIJKLMNO
ABCDEFGHIJKLMNOP
ABCDEFGHIJKLMNOPQ
ABCDEFGHIJKLMNOPQR
ABCDEFGHIJKLMNOPQRS
ABCDEFGHIJKLMNOPQRST
ABCDEFGHIJKLMNOPQRSTU
ABCDEFGHIJKLMNOPQRSTUV
ABCDEFGHIJKLMNOPQRSTUVW
ABCDEFGHIJKLMNOPQRSTUVWX
ABCDEFGHIJKLMNOPQRSTUVWXY
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

OPEN | RTS | DTR | Sending...

COM14:

```
ABCDEFGHIJKLMNOPQRSTUVW
ABCDEFGHIJKLMNOPQRSTUVWX
ABCDEFGHIJKLMNOPQRSTUVWXY
ABCDEFGHIJKLMNOPQRSTUVWXYZ
A
AB
ABC
ABCD
ABCDE
ABCDEF
ABCDEFG
ABCDEFGH
ABCDEFGHI
ABCDEFGHIJ
ABCDEFGHIJK
ABCDEFGHIJKL
ABCDEFGHIJKLM
ABCDEFGHIJKLMN
ABCDEFGHIJKLMNO
ABCDEFGHIJKLMNOP
ABCDEFGHIJKLMNOPQ
ABCDEFGHIJKLMNOPQR
ABCDEFGHIJKLMNOPQRS
ABCDEFGHIJKLMNOPQRST
ABCDEFGHIJKLMNOPQRSTU
ABCDEFGHIJKLMNOPQRSTUV
ABCDEFGHIJKLMNOPQRSTUVW
ABCDEFGHIJKLMNOPQRSTUVWX
ABCDEFGHIJKLMNOPQRSTUVWXY
ABCDEFGHIJKLMNOPQRSTUVWXYZ
A
AB
ABC
ABCD
AB
```

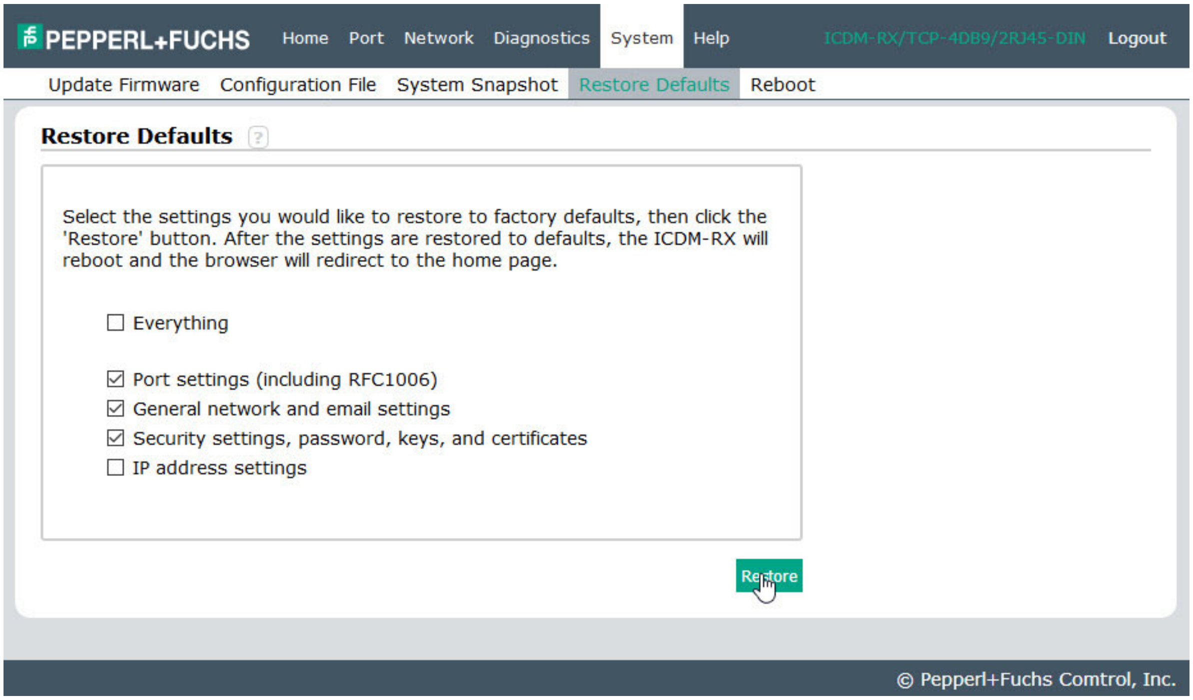
OPEN | RTS | DTR | Receiving...

11.5. Socket Mode Serial Port Testing

This procedure illustrates using Putty, which is available in PortVision DX. Optionally, you can use any other Winsock compatible application.

Note: *The following procedure starts with resetting ICDM-RX/TCP-16RJ45/2RJ45-PM to factory default values. You may want to save the ICDM-RX/TCP-16RJ45/2RJ45-PM socket configuration using PortVision DX - Saving a SocketServer Configuration File on Page 70.*

1. If necessary, install PortVision DX using *Installing PortVision DX* on Page 13 and scan the network to locate the ICDM-RX/TCP-16RJ45/2RJ45-PM that you want to test.
2. Right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM and click **Webpage**.
3. Click **System | Restore Defaults**.
4. Click the **Port settings** and **Security settings, password, keys, and certificates** options, and then the **Restore** button.



Restore Defaults

Select the settings you would like to restore to factory defaults, then click the 'Restore' button. After the settings are restored to defaults, the ICDM-RX will reboot and the browser will redirect to the home page.

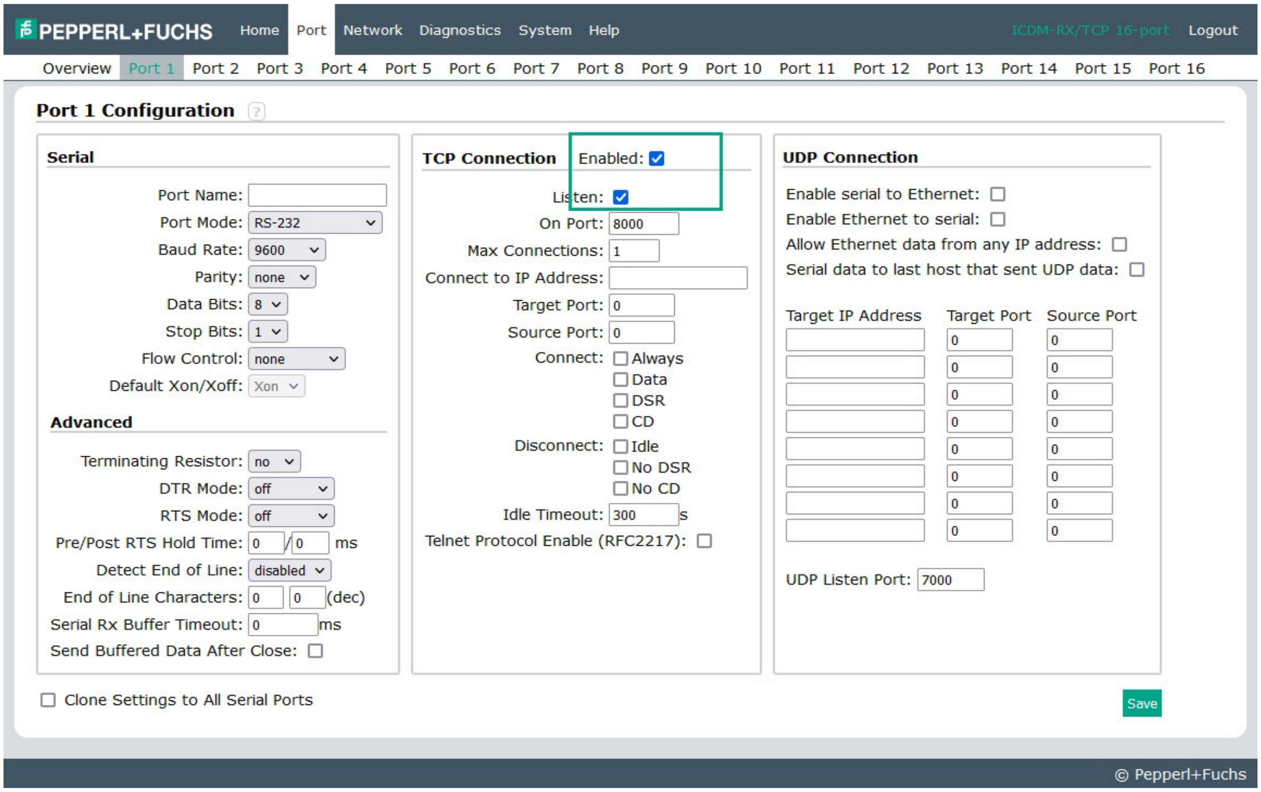
□ Everything

☑ Port settings (including RFC1006)
☑ General network and email settings
☑ Security settings, password, keys, and certificates
□ IP address settings

Note: *The ICDM-RX/TCP-16RJ45/2RJ45-PM will reboot.*

5. If necessary, re-open the web pages and click the port that you want to test.

6. Under the *TCP Connection Configuration* section, click the **Enable** option, and leave all other settings on this page at their default values.



Port 1 Configuration

Serial

Port Name:
Port Mode: RS-232
Baud Rate: 9600
Parity: none
Data Bits: 8
Stop Bits: 1
Flow Control: none
Default Xon/Xoff: Xon

Advanced

Terminating Resistor: no
DTR Mode: off
RTS Mode: off
Pre/Post RTS Hold Time: 0 / 0 ms
Detect End of Line: disabled
End of Line Characters: 0 0 (dec)
Serial Rx Buffer Timeout: 0 ms
Send Buffered Data After Close: □

TCP Connection Enabled: ☑

Listen: ☑
On Port: 8000
Max Connections: 1
Connect to IP Address:
Target Port: 0
Source Port: 0
Connect: □ Always □ Data □ DSR □ CD
Disconnect: □ Idle □ No DSR □ No CD
Idle Timeout: 300 s
Telnet Protocol Enable (RFC2217): □

UDP Connection

Enable serial to Ethernet: □
Enable Ethernet to serial: □
Allow Ethernet data from any IP address: □
Serial data to last host that sent UDP data: □

Target IP Address	Target Port	Source Port
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0
	0	0

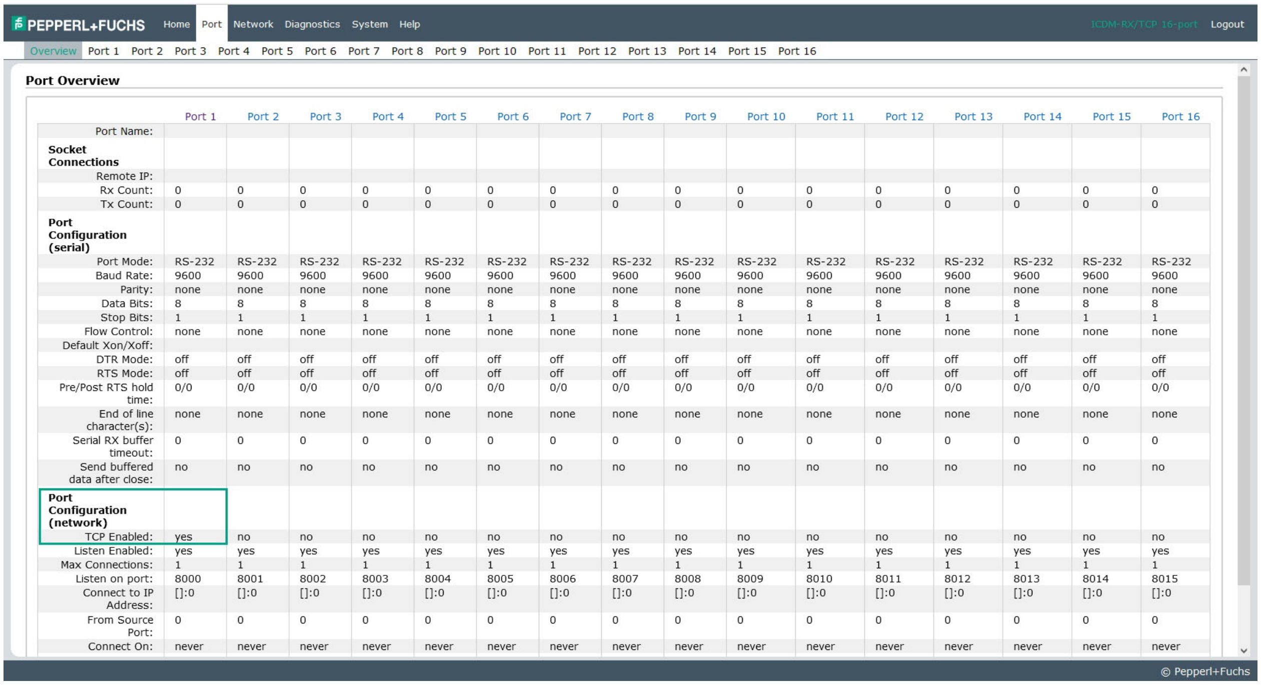
UDP Listen Port: 7000

□ Clone Settings to All Serial Ports

Note: *The Port number as it is needed later in this procedure. In this example, the port number is 8000.*

7. Click the **Save** button.

8. Click the **Overview** option and verify that the port has been enabled.



Port Overview

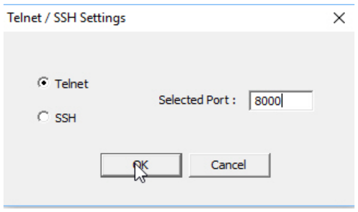
	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	Port 10	Port 11	Port 12	Port 13	Port 14	Port 15	Port 16
Port Name:																
Socket Connections																
Remote IP:																
Rx Count:	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tx Count:	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Port Configuration (serial)																
Port Mode:	RS-232	RS-232	RS-232	RS-232	RS-232	RS-232	RS-232	RS-232	RS-232	RS-232	RS-232	RS-232	RS-232	RS-232	RS-232	RS-232
Baud Rate:	9600	9600	9600	9600	9600	9600	9600	9600	9600	9600	9600	9600	9600	9600	9600	9600
Parity:	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none
Data Bits:	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
Stop Bits:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Flow Control:	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none
Default Xon/Xoff:																
DTR Mode:	off	off	off	off	off	off	off	off	off	off	off	off	off	off	off	off
RTS Mode:	off	off	off	off	off	off	off	off	off	off	off	off	off	off	off	off
Pre/Post RTS hold time:	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
End of line character(s):	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none	none
Serial RX buffer timeout:	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Send buffered data after close:	no	no	no	no	no	no	no	no	no	no	no	no	no	no	no	no
Port Configuration (network)																
TCP Enabled:	yes	no	no	no	no	no	no	no	no	no	no	no	no	no	no	no
Listen Enabled:	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Max Connections:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Listen on port:	8000	8001	8002	8003	8004	8005	8006	8007	8008	8009	8010	8011	8012	8013	8014	8015
Connect to IP Address:	[]:0	[]:0	[]:0	[]:0	[]:0	[]:0	[]:0	[]:0	[]:0	[]:0	[]:0	[]:0	[]:0	[]:0	[]:0	[]:0
From Source Port:	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Connect On:	never	never	never	never	never	never	never	never	never	never	never	never	never	never	never	never

9. Leave the web page open.

10. Attach the loopback plug that was shipped with the ICDM-RX/TCP-16RJ45/2RJ45-PM to the serial port of the ICDM-RX/TCP-16RJ45/2RJ45-PM. See *Connecting Serial Devices* on Page 76 if you need to build a loopback plug.

11. Right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM and click **Telnet / SSH Session**.

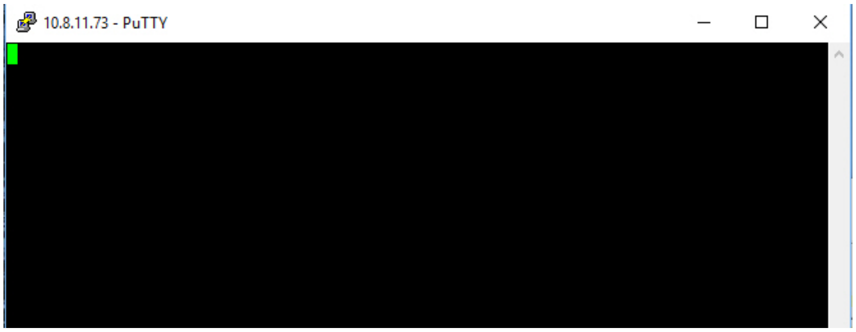
12. Enter the socket number of the port that you are testing and click **Ok**.



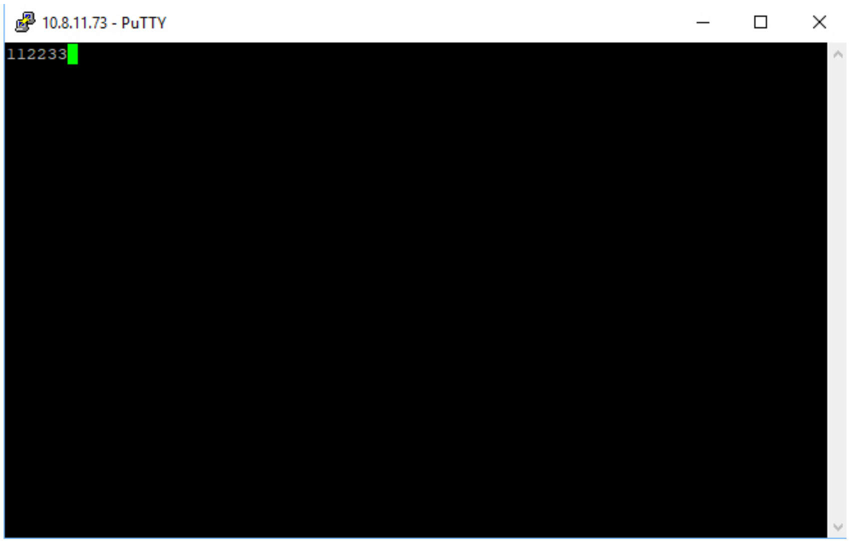
● Telnet
○ SSH

Selected Port : 8000

PuTTY loads.



13. Type 123.

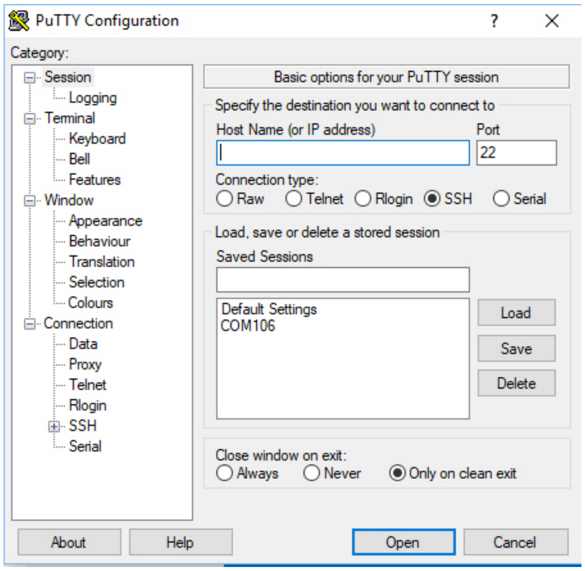


```
112233
```

Note: *If 112233 displays, you need to disable local echo. Use the following steps to disable local echo.*

a. Close the Telnet session.

b. Click **Tools | Applications | PuTTY**.



Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

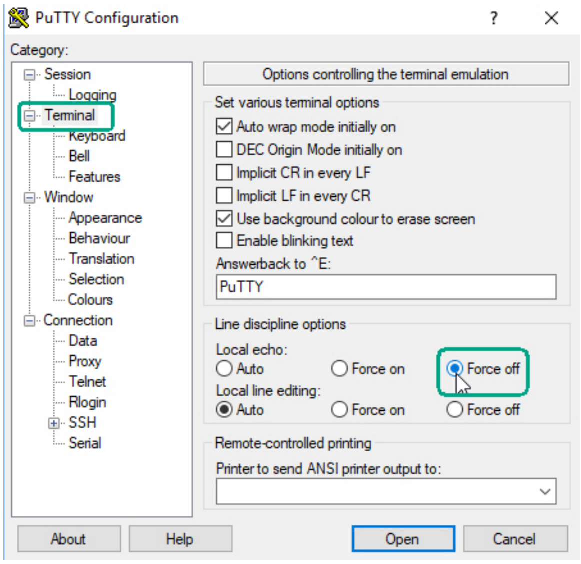
Load, save or delete a stored session

Saved Sessions:

Default Settings
COM106

Close window on exit: ○ Always ○ Never ● Only on clean exit

c. Click **Terminal** and click **Force off** for the *Local echo* option.



Set various terminal options

☑ Auto wrap mode initially on
□ DEC Origin Mode initially on
□ Implicit CR in every LF
□ Implicit LF in every CR
☑ Use background colour to erase screen
□ Enable blinking text

Answerback to ^E: PuTTY

Line discipline options

Local echo: ○ Auto ○ Force on ● Force off

Local line editing: ● Auto ○ Force on ○ Force off

Remote-controlled printing

Printer to send ANSI printer output to:

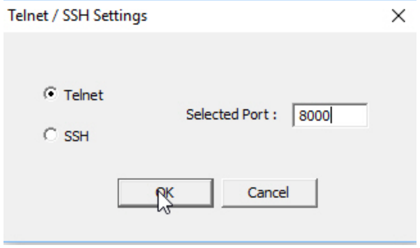
d. Return to the **Session** menu, highlight **Default Settings** and then click **Save**.

e. Click **Cancel** to close PuTTY.

f. Close the telnet (PuTTY) session that you opened from PortVision DX.

g. Re-open the telnet session by right-clicking the ICDM-RX/TCP-16RJ45/2RJ45-PM, and select the **Telnet / SSH Session** option.

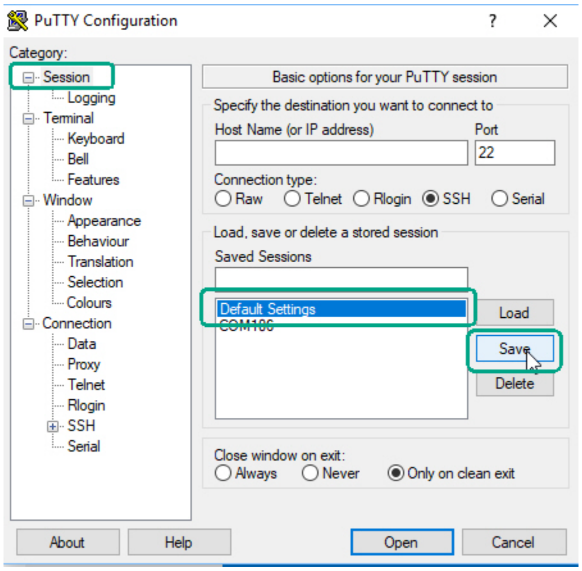
h. Enter the Socket Port number and then click **Ok**.



● Telnet

○ SSH

Selected Port : 8000



Specify the destination you want to connect to

Host Name (or IP address)

Port 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

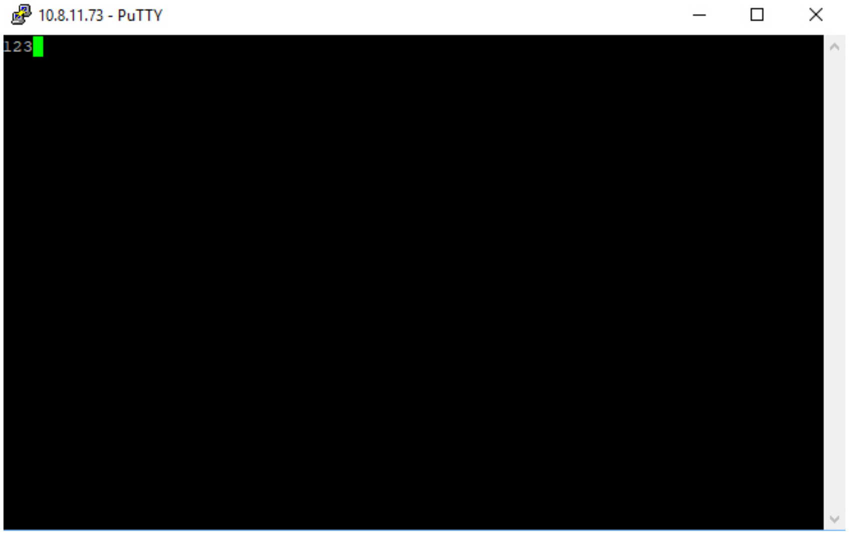
Load, save or delete a stored session

Saved Sessions

Default Settings
COM106

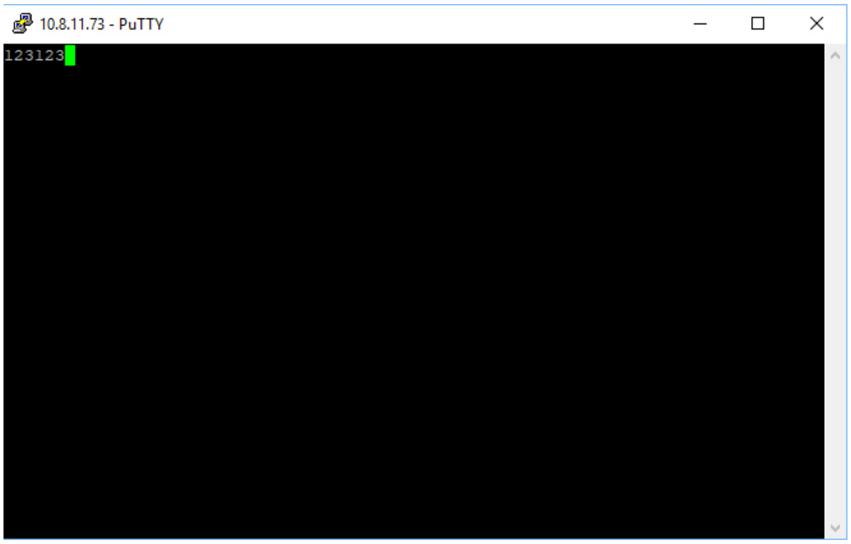
Close window on exit: ○ Always ○ Never ● Only on clean exit

i. Enter **123**, single digits should appear.



```
10.8.11.73 - PuTTY
123
```

14. Remove the loopback plug and type **abc**. No characters should display because the return path is open.
15. Re-attach the loopback plug, type **abc**, and the characters should appear.



```
10.8.11.73 - PuTTY
123123
```

16. If you want to test additional ports, simply repeat this procedure on that port or ports.
17. Remove the loopback plug from the serial port and attach your serial device.

    You may need to set the serial parameters as necessary to match your attached equipment.

11.6. Daisy-Chaining ICDM-RX/TCP-16RJ45/2RJ45-PM With Dual Ethernet Ports

The ICDM-RX/TCP-16RJ45/2RJ45-PM models with dual Ethernet ports follow the IEEE specifications for standard Ethernet 10/100BASE-TX topologies.

When using the **E1** and **E2** ports, the ICDM-RX/TCP-16RJ45/2RJ45-PM is classified as a switch. When using the **UP** port only, it is a simple end node device.

The maximum number of daisy-chained ICDM-RX/TCP-16RJ45/2RJ45-PM units, and the maximum distance between units is based on the Ethernet standards and will be determined by your own environment and the conformity of your network to these standards.

Pepperl+Fuchs has tested with seven ICDM-RX/TCP-16RJ45/2RJ45-PM units daisy-chained together using 10 foot CAT5 cables, but this is not the theoretical limit. You may experience a performance hit on the devices at the end of the chain, so it is recommended that you overload and test for performance in your environment. The OS and the application may also limit the total number of ports that may be installed.

Following are some quick guidelines and URLs of additional information. Note that standards and URLs do occasionally change.

- Ethernet 10BASE-T Rules
  - The maximum number of repeater hops is four.
  - You can use Category 3 or 5 twisted-pair 10BASE-T cables.
  - The maximum length of each cable is 100m (328ft).

    Note: *Category 3 or 5 twisted pair cables look the same as telephone cables but they are not the same. The network will not work if telephone cables are used to connect the equipment.*
- Fast Ethernet 100BASE-TX rules
  - The maximum number of repeater hops is two (for a Class II hub). A Class II hub can be connected directly to one other Class II Fast Ethernet hub. A Class I hub cannot be connected directly to another Fast Ethernet hub.
  - You must use Category 5 twisted-pair 100BASE-TX cables.
  - The maximum length of each twisted-pair cable is 100m (328ft).
  - The total length of twisted-pair cabling (across directly connected hubs) must not exceed 205m (672ft).

    Note: *Category 5 twisted pair cables look the same as telephone cables but they are not the same. The network will not work if telephone cables are used to connect the equipment.*
- IEEE 802.3 specification: A network using repeaters between communicating stations (PCs) is subject to the 5-4-3 rule of repeater placement on the network:
  - Five segments connected on the network.
  - Four repeaters.
  - Three segments of the 5 segments can have stations connected. The other two segments must be inter-repeater link segments with no stations connected.

    Additional information may be found by searching the web.

11.7. ICDM-RX/TCP-16RJ45/2RJ45-PM LEDs

The ICDM-RX/TCP-16RJ45/2RJ45-PM has network and port LEDs to indicate status. This subsection discusses:

- *TX/RX LEDs*
- *Network and Device LEDs* on Page 120

11.7.1.TX/RX LEDs

The RX (yellow) and TX (green) LEDs function accordingly when the cable is attached properly to a serial device.

LED	Mode	Description	LED Status
RX (Green)	RS-232	No valid RS-232 device is connected	Always off
		Valid RS-232 device is connected but no data transmission is occurring	On
		Data being received LED blinks	LED blinks
	RS-422/485	No data being received	Always off
		Data being received LED blinks	LED blinks
	No mode	No mode selected	Always off
TX (Yellow)	RS-232/422/485	No data being transmitted	Always off
		Data being transmitted LED blinks	LED blinks

- After power cycling the ICDM-RX/TCP-16RJ45/2RJ45-PM, the RX/TX LEDs are off.
- The LEDs do not function as described until the port has been opened by an application. You can use Test Terminal in PortVision DX to open a port or ports if you want to test a port or ports (*Testing Ports Using Test Terminal* on Page 106).

11.7.2.Network and Device LEDs

The LEDs indicate that the default ICDM-RX/TCP-16RJ45/2RJ45-PM application, SocketServer is running or after driver installation, that the NS-Link driver loads. If you have loaded PortVision DX, you can check the ICDM-RX/TCP-16RJ45/2RJ45-PM status on-line.

- If the Status LED on the ICDM-RX/TCP-16RJ45/2RJ45-PM is lit, it indicates the ICDM-RX/TCP-16RJ45/2RJ45-PM has power and it has completed the boot cycle.

  The Status LED flashes while booting and it takes approximately 15 seconds for the Bootloader to complete the cycle. When the Bootloader completes the cycle, the LED has a solid, steady light that blinks approximately every 10 seconds.
- The green Ethernet LED indicates that a link has been established and the yellow Ethernet LED indicates activity

11.8. Removing ICDM-RX/TCP-16RJ45/2RJ45-PM Security Features

When presented with an ICDM-RX/TCP-16RJ45/2RJ45-PM that has had all security options set and the user is unaware of what the settings are, the restoring of an ICDM-RX/TCP-16RJ45/2RJ45-PM can be very difficult.

It may be necessary to use the ICDM-RX/TCP-16RJ45/2RJ45-PM debug dongle provided with the *Software Developers Kit* (SDK) or return the ICDM-RX/TCP-16RJ45/2RJ45-PM to Pepperl+Fuchs after obtaining an return material authorization (RMA) so that Pepperl+Fuchs can re-flash the ICDM-RX/TCP-16RJ45/2RJ45-PM with default values.

One of the following two conditions must be true, so that you can remove the security settings from the ICDM-RX/TCP-16RJ45/2RJ45-PM.

- Serial connection using Port 1 to access RedBoot:
    - Bootloader timeout set to value greater than 10 seconds (default is 15 seconds).
    - A known good null modem cable.
    - A COM port on PC/Laptop.
- Bootloader *Command Console* using an Ethernet connection
    - No password or a known password.
    - A known or discoverable IP address.
    - A utility such as *Angry IP Scanner* from www.angryip.org may be used to discover IP addresses. If the IP range is unknown, a full scan from 0.0.0.1 to 255.255.255.255 may take a long time.
    - An Ethernet cable.
    - A PC/Laptop with a telnet application installed such as PuTTY included in PortVision DX.

11.8.1.Serial Connection Method

Use the following procedure to set up serial connection with a terminal server program (for example, Test Terminal (WCom2), HyperTerminal or Minicom) and the ICDM-RX/TCP-16RJ45/2RJ45-PM.

Note: *Optionally, you can use PuTTY, which is included in PortVision DX under the* **Tools >Applications > PuTTY** *menu.*

1. Connect a null-modem cable from an available COM port on your PC to **Port 1** on the ICDM-RX/TCP-16RJ45/2RJ45-PM.

   Note: *See Connecting Serial Devices on Page 76 to build a null-modem cable.*

2. Configure the terminal server program to the following values:
   - Bits per second = 57600
   - Data bits = 8
   - Parity = None
   - Stop bits = 1
   - Flow control = None

3. Reset the ICDM-RX/TCP-16RJ45/2RJ45-PM.

   Note: *Depending on the model, disconnect and reconnect the power cable (external power supply and no power switch) or turn the power switch on and then off (internal power supply).*

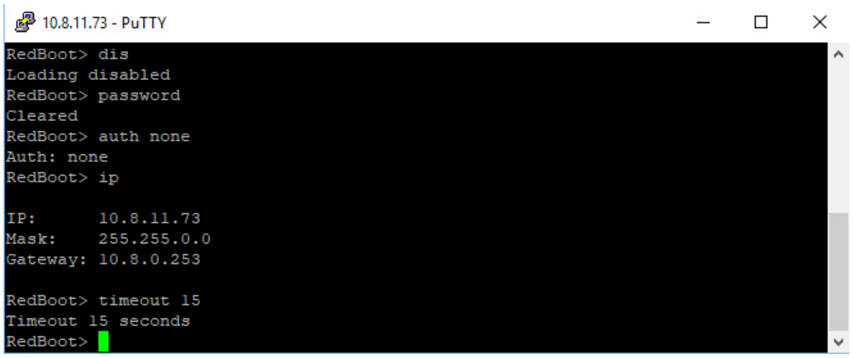
4. Immediately type **#!DM** and press **Enter** in the terminal program.

5. At the **RedBoot>** prompt, type **dis**, and press **Enter**.

   Note: *If you do not disable the loading feature of the Bootloader within the time-out period (default is fifteen seconds), an application will be loaded from flash and started. If this happens, repeat Steps 3 through 5. The* ***#!DM*** *command is the only case-sensitive command and must be in uppercase.*

6. Enter **password** and press **Enter**, which clears the existing password.
7. Enter **auth none** and press **Enter**, which removes the authentication level.
8. If you do not know the IP address, enter **ip** and press **Enter**.
9. Enter **timeout 15** and press **Enter**, which sets a reasonable timeout value.

   Note: *If the Bootloader timeout has been set too low to allow console port access, and the IP address cannot be discovered, then the ICDM-RX/TCP-16RJ45/2RJ45-PM must be returned to Pepperl+Fuchs for re-flashing.*

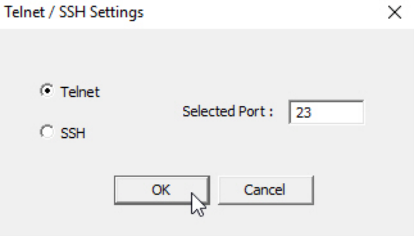


```
RedBoot> dis
Loading disabled
RedBoot> password
Cleared
RedBoot> auth none
Auth: none
RedBoot> ip

IP:      10.8.11.73
Mask:    255.255.0.0
Gateway: 10.8.0.253

RedBoot> timeout 15
Timeout 15 seconds
RedBoot>
```

10. Connect the ICDM-RX/TCP-16RJ45/2RJ45-PM directly to the PC/laptop running PortVision DX.

    Note: *If necessary, see Installing PortVision DX on Page 13.*

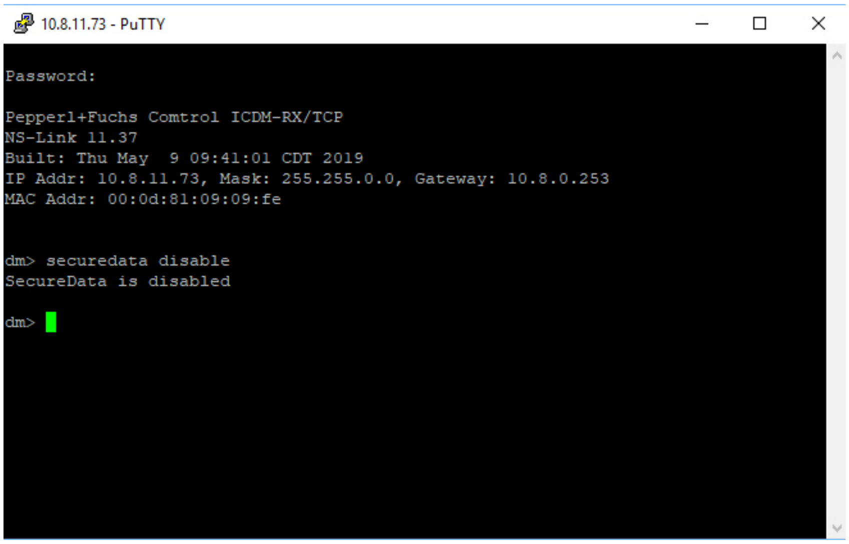
11. Open PortVision DX.
12. Scan the network so that PortVision DX discovers the ICDM-RX/TCP-16RJ45/2RJ45-PM.
13. Right-click the ICDM-RX/TCP-16RJ45/2RJ45-PM and then click **Telnet/SSH Session**.
14. Click **Telnet**, leave Port 23 as the *Selected Port* and click **Ok**



● Telnet
○ SSH
Selected Port : 23

15. Press **Enter** at the *Password* prompt.
16. Enter **secureconf disable** and press **Enter**.

17. Enter **securedata disable** and press **Enter**.



```
Password:

Pepperl+Fuchs Comtrol ICDM-RX/TCP
NS-Link 11.37
Built: Thu May  9 09:41:01 CDT 2019
IP Addr: 10.8.11.73, Mask: 255.255.0.0, Gateway: 10.8.0.253
MAC Addr: 00:0d:81:09:09:fe


dm> securedata disable
SecureData is disabled

dm>
```

FACTORY AUTOMATION – SENSING YOUR NEEDS

Worldwide Headquarters
Pepperl+Fuchs Group
68307 Mannheim · Germany
Tel. +49 621 776-0
E-mail: info@de.pepperl-fuchs.com

USA Headquarters
Pepperl+Fuchs Inc.
Twinsburg, Ohio 44087 · USA
Tel. +1 330 4253555
E-mail: sales@us.pepperl-fuchs.com

Asia Pacific Headquarters
Pepperl+Fuchs Pte Ltd.
Company Registration No. 199003130E
Singapore 139942
Tel. +65 67799091
E-mail: sales@sg.pepperl-fuchs.com

www.pepperl-fuchs.com

PEPPERL+FUCHS
SENSING YOUR NEEDS